OPENTEXT

OCTOBER 2013

Are Big Files Big Problems?

Breaking down file transfer challenges with Managed File Transfer

Files are getting bigger and the sharing of information is getting more complex. Organizations today are transferring information not only between local employees but global departments, partners, customers, legal providers, and more on a daily basis. This transfer of information needs not only to be easy, but efficient, secure, and auditable. This paper discusses the challenges associated with file transfer solutions and how Managed File Transfer solutions solve these problems.

Table of Contents

Is Your File Transfer Solution Enterprise-Ready? 3

The Challenges of Transferring Files 4

The Challenges with Existing File Transfer Methods 5

FTP sites are complex and lack security 5

Email is ubiquitous but not optimal for large files 5

Internet file sharing lacks enterprise security 6

Physical delivery is slow and insecure 6

Breaking Down File Transfer Challenges with Managed File Transfer. 7

MFT: The Next-Generation Platform for Content Sharing 8

OpenText Managed File Transfer is an integral component of the Information Exchange (IX) suite that OpenText offers to help organizations execute on comprehensive Enterprise Information Management strategies. IX capabilities facilitate the efficient, secure, and compliant exchange of information inside and outside of the enterprise.

Is Your File Transfer Solution Enterprise-Ready?

The Internet has dissolved geographical barriers and connected us in ways that were unimaginable a generation ago. Thousands of miles of fiber optic lines, undersea cables, and fleets of orbiting satellites have connected continents in exciting new ways, and, in the process, have created an information superhighway that enables vast amounts of data to flow. And the capital has followed.

The global network has leveled the playing field to an astonishing degree. Today, a manu- facturing company headquartered in Chicago can collaborate with engineers in Mumbai, factory foremen in Shanghai, advertising executives in London, and bankers in Dubai. The Internet has opened new markets, fostered greater competition, and redefined the business enterprise. What used to be a corporate office with cubicles of users is now a complex global network of partners, customers, employees, and systems—all requiring specific access, control, and security over information assets.

However, while the Internet has become indispensable to modern businesses, it has also created some unique challenges. In particular, people have struggled to cope with the sheer amount of data being generated. According to a recent forecast by analysts at IDC, the amount of data created around the world in 2011 will approach 2 zettabytes (or 2 million petabytes).

And the size of individual files is also growing. Thanks to ever-improving hardware and software, companies are cramming more and more data into their files. Whether it's an AutoCAD® drawing of a new product, a three-dimensional view of an oil field, or a very large PDF or PowerPoint® presentation, companies are banking on the incredible power of computers today to quickly chew through gigabytes of data to give them a competitive edge.

The growth of large files is particularly evident in the engineering field, which has historically been very dependent on paper. Today, that near total reliance on paper is thawing, and engineering firms are shifting much of their work to computers and digital formats, which has stopped the endless scanning and printing that used to go into sharing design or product information with stakeholders. But this has created other problems.

With today's cheap and powerful 64-bit workstations, companies are well equipped to deal with large engineering files. However, the business processes that are used to distribute the files in a secure, efficient, and compliant fashion often leaves much to be desired.

The Internet has opened new markets, fostered greater competition, and redefined the business enterprise. What used to be a corporate office with cubicles of users is now a complex global network of partners, customers, employees, and systems—all requiring specific access, control, and security over information assets.

The Challenges of Transferring Files

The democratization of the workforce has combined with the never-ending increase in data and file sizes to put the crunch on file transfer activities. When a network is set up inside the firewall, employees are often free to share files through a common drive accessible over the LAN, which is easy to use and offers good performance but suffers a bit when it comes to security and central control.

However, once a file travels outside the firewall, little internal security transgressions are magnified into major potential problems. For companies that need to communicate with outside stakeholders, such as telecommuters, contractors, lawyers, directors, suppliers, customers, and various other entities, a seemingly minor flaw in file transfer technique could balloon into a giant headache.

There are multiple ways that a bad file transfer could cost a company. For starters, any company in a regulated industry should make sure they have adequate security and compliance controls in place to protect sensitive data. Depending on the industry, a company will be required to encrypt their transmittals per the terms of PCI DSS, HIPAA, SOX, J-SOX, Basel II, GLBA, and others. Companies that do business with the U.S. government will need a solution that's FIPS 140-2 certified.

In addition to encryption requirements, many of these regulations also require strong auditing capabilities. Without a detailed log that lists all file transfer participants and activities, a company may not survive an audit for compliance with their pertinent industry regulation. Failure to adhere to the any compliance requirements could result in fines and increased visits from auditors.

Intellectual Property (IP) and trade secrets are also at play here. The large files that are shared among manufacturers, designers, and engineering and architectural firms often contain extremely valuable IP that warrants special handling. Just as an employee for one of these firms would never think of posting the data on a public website or leaving it lying on a park bench, they should also never use an unsecured method of transmitting them electronically. Unfortunately, too many of them do.

The Challenges with Existing File Transfer Methods

FTP sites are complex and lack security

The engineer could send the file via File Transfer Protocol (FTP). FTP use has flourished in recent years, in large part because there is no size limit, making it a feasible choice for files ranging from 2GB to 50GB. Many users around the world can collaborate with a single FTP server, and there is rudimentary tracking.

But FTP has some fatal flaws that make it a very poor choice for any organizations that value security, ease-of-use, and performance. For starters, it's not an effective ad-hoc solution. It takes time to set up an FTP server, and there is client software to distribute, install, and configure. Firewalls must be negotiated. This is simply too much hassle for an ad-hoc file distribution situation.

But the biggest problem with FTP is its utter lack of security. It may sound surprising, but user names and passwords are sent as plain text over the FTP protocol, making the contents of an FTP session susceptible to an entry-level hacker equipped with a sniffer program. And while FTP servers do typically log file transfer activity, it can be a challenge to interpret this data to extract meaningful information.

There may also be a performance penalty with FTP. It may take six to eight hours to send a 20 GB file over FTP. Without checkpoint restarts and other Quality of Service (QoS) mechanisms, any hiccup in the network can doom a long FTP session, and the sender may not even realize the file was not successfully transmitted.

Email is ubiquitous but not optimal for large files

Email would be the preferred mechanism for distributing files. After all, it is well-adopted, easy to use, and fairly reliable. However, it simply wouldn't work for our engineer's 10GB AutoCAD file. For example, the default attachment size limit in Microsoft® Exchange, the most widely used corporate email server, is a paltry 10MB. Some organizations increase this, but administrators must take pains to ensure the larger files don't cause other problems, such as creating a bottleneck in the network.

Some public email offerings support larger attachment sizes. Google's Gmail service, for example, will support files up to 25 MB. Even in best-case scenarios, emails with large attachments may be blocked at the server anyway, as MIME encoding typically increases an attachment by about 30 percent.

To get around the file size limits of email servers (and avoid MIME's tax), users will sometimes break up large files into smaller chunks which can be reassembled at their destination. Free file splitting software abounds on the web, but this can be a hassle to use and confounds the ability to track files and the people who consume them.

Encryption can be used with email, but it can be difficult to set up, and is not universally supported with all email clients. In the end, email is simply not a feasible choice when it comes to secure ad hoc file distribution—in any industry.

Internet file sharing lacks enterprise security

Our engineer may try using one of the various web-based file sharing services that have popped up over the years. Firms like YouSendIt.com™ provide file transfer via email offloading, whereby the recipient of a file receives an email that contains a web link where they can download the file. The integration with email makes it easy to use and, therefore, good for ad-hoc, unplanned file transfers. Some services provide encryption, which should always be used when sending critical business data over the Internet.

However, there are some downsides to public file sharing services that make them less than ideal for business users. For starters, files bigger than 2GB can't be distributed via HTTP-based services. While some of these outside services provide auditing and reporting functions, they will not be ideal for organizations that want to maintain strict control over their data. An overall lack of integration with an enterprise's existing security systems leaves too much outside of its control.

Physical delivery is slow and insecure

As a last resort, the engineer may try to send his large AutoCAD file using physical media, such as a DVDs, 8 MM tape, or even large-capacity USB memory sticks, and the mail. This has been the preferred method when hundreds of very large files, such as three-dimensional drawings of an undersea oil field or a VMware image of an entire operating system instance, need to be delivered across the globe.

The biggest problems with courier services have to do with speed and security. It can take a week or more to send a file from a remote field office half-way across the globe to company headquarters. And even if the data is encrypted, the break in the chain of custody means the data could be compromised.

The lack of a digital trail starts to cause problems when truly massive amounts of data are split up into dozens or hundreds of files. In this situation, it's up to the recipient to piece together the files into the correct order. In the end, if the data is time-sensitive and worth perhaps millions of dollars—which is commonplace in the oil and gas exploration business—it simply doesn't make sense to waste time with a delivery service. In this day and age, there are much better methods of transferring large data sets across the network in a secure fashion.

Breaking Down File Transfer Challenges with Managed File Transfer

A Managed File Transfer (MFT) solution can alleviate all of these problems that are associated with the secure distribution of files in both ad-hoc and scheduled environments. Over the last few years, the MFT product category has grown and, today, many MFT vendors' offerings resemble frameworks that users can customize and adapt to suit their particular file transfer needs.

While features vary from one MFT solution to another, they typically deliver a common set of core capabilities, including:

- Strong security, via end-to-end encryption of contents and authentication of users. SFTP, which uses Secure Shell (SSH) encryption, is becoming the standard protocol for MFT, but FTPS, which uses SSL, and even PGP-based encryption are also widely used. Integration with user directories (Active Directory or LDAP) provide enterprise-level authentication using either passwords or certificates.
- Auditing, through detailed logging and reporting. Most FTP products track usage, but the better MFT products will provide reporting tools that simplify the task for users and auditors.
- Centralized management, including alerts. The capability to view all MFT activity from one console is critical in enterprise settings with hundreds or thousands of connections and users.
- Performance and guaranteed delivery. QoS features such as check-point restarts and file acceleration ensures MFT users that files are delivered quickly every time.
- Automation and business process management. The capability to kick off a business process upon the completion of a file transfer task is a common feature of most MFT products.

Several other features are common to some but not all MFT solutions, such as email offloading, which is particularly effective for ad-hoc MFT. Email offloading allows users to send large files using regular email. Instead of distributing the file as an attachment, the MFT solution strips out the file, replaces it with a web link, and sends the file using a separate channel. Recipients can download the file by clicking on the web link. In addition to eliminating the need for any special MFT client software, email offloading reduces the burden on the email server.

Another feature found in some MFT solutions is lifecycle management of content, including check-in and check-out of content. This feature makes it easier for an organization to control revisions to files. It's also important for narrowing the risk of IP loss. Some MFT offerings utilize proxies to further protect internal networks from outside threats.

When email offloading is not being used, most MFT solutions use either a proprietary client that downloads to the PC or workstation or a web-based client. In general, PC-based clients usually offer more capabilities, but web-based clients are usually easier to use. However, MFT solutions that utilize HTTPS are faced with a 2GB limit for file transfers, which leaves the door open for more specialized, high-performance MFT solutions.

Use of proprietary protocols can eliminate some of the size and speed restrictions imposed by the TCP/IP protocol. They typically are faster than FTP-based transfers, and usually provide more advanced proof of delivery and checkpoint restart mechanisms. While proprietary MFT solutions can boost performance, they typically require all participants to have specialized clients installed. Often, MFT solutions that use high-performance proprietary protocols will also feature support for FTPS or SFTP for communicating with partners who haven't installed the client.

MFT: The Next-Generation Platform for Content Sharing

In the end, MFT becomes the clear file transfer method of choice for our engineer with the 10GB AutoCAD file. The engineer now has the advantage of knowing that, by adopting an MFT solution, he's adopted the current best practice for ensuring the integrity and security of critical information.

Companies in every industry are faced with the same problem: how do I securely distribute files with my co-workers and business partners? Many people have gravitated to FTP as a result of its unlimited file size limit. But there is a growing realization that complete lack of encryption and weak auditing in FTP make it a liability, not an asset, when it comes to file transfer activities.

Likewise, the stopgap solutions provided by Internet-based file transfer services and delivery of physical media by courier do not satisfy the demands for a secure, fast, and auditable file transfer solution. With MFT, companies are realizing they have a solid backbone on which to base their global information sharing activities—for now and into the future.

About OpenText

OpenText provides Enterprise Information Management software that enables companies of all sizes and industries to manage, secure, and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit: www.opentext.com.

opentext.com/ixsuite

NORTH AMERICA +1 800 304 2727 ■ UNITED STATES: 1 425 455 6000
EUROPE +31 (0)23 565 2333 ■ AUSTRALIA: +61 2 9026 3480