WHITE PAPER

Making File Transfer Easier, Compliant and More Secure

An Osterman Research White Paper

Published February 2012

SPONSORED BY

FileCatalyst®
reinventing file transfer

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

Email is the primary file-transfer solution in just about every organization. For example, an Osterman Research survey[i] found that only 22% of emails contain attachments, but more than 90% of the bits flowing through an email system are accounted for by these attachments. The reasons for using email as a file-transfer solution are simple: email is ubiquitous, it is based on industry standards, and it is very easy to use as a drag-and-drop file transfer utility.

However, email was never designed as a file-transfer system and users and organizations suffer from using it this way:

- Email systems become bloated with content, they become more difficult and more time-consuming for IT staffers to manage, and the costs of email management are much higher than they should be.
- Content sent through email is largely unmanaged, offering senders no assurance that recipients have received attachments, that the content was not modified by the recipient or some intermediate party along the way, and with no control over access to it.
- Departments and workgroups cannot gain access to this shared data unless they happen to be on the sender's list of recipients.
- Organizations experience much greater exposure to data breaches and the associated financial and other consequences of losing control of sensitive corporate data.

Individually focused solutions, many of which operate in the cloud, can provide good functionality for users as an alternate method for sending files, but many lack corporate governance capabilities that will allow centralized management and control over content.

Individually focused solutions, many of which operate in the cloud, can provide good functionality for users as an alternate method for sending files, but many lack corporate governance capabilities that will allow centralized management and control over content.

While many organizations have legacy FTP systems in place to act as an alternate channel for sending files, these systems suffer from lack of governance and lack of security, not to mention the fact that IT must manage this legacy infrastructure that most users don't employ anyway.

Other file-transfer alternatives to email, such as physical delivery, are very expensive and much slower.

KEY TAKEAWAYS

Consequently, what organizations need is:

- A way for users to send files independently of email that will address the critical requirements for corporate governance and information security. These types of transfers are truly legitimate, business-oriented activities that don't come on a regularly scheduled basis – performing these transfers is essential to user productivity.

- Moreover, such a system must integrate seamlessly into the way that individuals work if they are to use it. This includes the increasing need to work from either personal or work-provisioned smartphones and tablets.

- The solution should allow internal users to share corporate files across organizational boundaries without having to rely on IT to provision licenses.

- Finally, such a solution should ideally be less expensive than using email and other solutions for file transfer in order to achieve additional benefits.

ABOUT THIS WHITE PAPER

This white paper discusses the critical importance of finding a better alternative to email as a file-sharing mechanism. It also provides information on the sponsor of this white paper – FileCatalyst – and its relevant solutions.

The Current State of File Transfer

HOW CONTENT IS SENT TODAY

Most email users employ email as the primary way to send files like word processing documents, spreadsheets, presentations, images and other content. In fact, Osterman Research has calculated that more than 90% of the bits that are sent through email systems are actually attachments to email messages and not the messages themselves. There are a number of good reasons for using email as the default file-transfer mechanism, including:

- Email is very easy to use and requires minimal training in order to send attachments.

- Email systems are built on industry standards and provide users with a high degree of assurance that their emails can be received and opened by recipients (albeit without proof that their attachments have *actually* been received by the recipients).

- Virtually every corporate user and consumer has email available on a wide range of platforms (desktop client at work or home, laptop, browser, smartphone, tablet, etc.)

As a result, email has become the default way to send files in almost all organizations. While other tools – such as FTP systems, instant messaging and physical delivery – are used to send electronic files, consumer file-sharing applications, email continues to be the primary platform that individuals use to send electronic content.

CHANGING TRENDS IN FILE TRANSFER

There are a number of important trends taking place in the context of how attachments are managed:

- **Attachments are getting larger**
  Attachments are becoming larger as users create more content: word processing documents, spreadsheets, videos, presentations, PDF files, and other materials. This is particularly true as the use of video increases for training and other purposes, and as

content authoring tools become more sophisticated.

- **Data security is becoming more important**
  Another important trend in managing content is the growing importance of data breach prevention. Motivated by compliance regulations, growing concerns over data leaks, and protection of intellectual property, IT needs greater visibility into who is transferring content and the types of content that are sent.

- **File-sharing and synchronization applications are becoming more popular**
  There is growing use of file-sharing and data synchronization applications, such as Dropbox and SugarSync, that are very useful, but that create the potential for leakage of intellectual property and other data breaches.

- **Organizations are more globally distributed**
  As organizations, their business partners and their supply chains become more globally distributed, there is a need to improve the speed and the reliability of file transfer for sharing critical documents, such as design documents between a company in North America and its manufacturing partners in Asia.

- **Content lifecycle management is also more important**
  Increasingly, IT and individual users need better visibility into how content is sent, who has access to it, the assurance of its delivery, and how long content is available.

- **Email is being used more**
  Although there are many alternatives for communication, collaboration and file transfer, the use of email continues to increase. For example, a September 2011 Osterman Research survey found that the average email user sends and receives 145 emails on a typical workday. Moreover, 42% of those surveyed reported that they are using email more than they did 12 months earlier, while only 10% reported using email less over the same time period.

- **Telework and remote work are becoming more common**
  Employees, contractors and temporary workers are becoming more distributed as companies implement telework/work-from-home policies to reduce the costs of rent and other expenses associated with providing employees office space. The result is that employees who can no longer work together physically now rely more on the sharing of documents by email in order to collaborate on projects.

Content on FTP systems is often unmanaged, leading to corporate governance problems. It can sit on an FTP server for many years, leading to potential data breaches from unauthorized parties outside a company, or unauthorized access to individuals inside the company.

Closely related to this is the shift to BYOD (Bring Your Own Device) mentality among employees who increasingly use personal smartphones and tablets to do their work.

The Problem With Current File Transfer Methods

CONSUMER FILE-SHARING APPS LACK CORPORATE GOVERNANCE

Another issue is that IT typically lacks control over content that is sent outside an organization (and often within it), because unsanctioned use of various free solutions for transferring files is prevalent behind corporate firewalls. While many of these consumer-focused solutions are quite useful and work as advertised, they often do not provide IT with the tools to centrally manage corporate content. In the typical scenario, while IT may be charged with archiving or otherwise managing content for legal, regulatory or other purposes, it lacks the ability to fully control the flow of information sent through email. Further, IT has almost no visibility into content that is sent via means other than email, such as cloud-based file transfer tools, overnight packages, USB drives, personal email, etc.

Related to this problem is that performing audits on or delivery verification of externally sent content is difficult in many cases. For example, if a user sends a time-sensitive proposal to a recipient through email, usually the only way to verify the delivery of this content is to send another email or call the recipient. Most email systems do not provide the ability to track the flow of content from sender to recipient throughout the entire transfer process.

FTP SYSTEMS ARE NOT AS SECURE AS THEY SHOULD BE

The venerable FTP systems that have been deployed in most organizations are useful for sending large files, but they suffer from two serious problems:

- First, they lack security because so many users share login credentials for the occasional large file transfers for which they use these systems.

- Second, content on FTP systems is often unmanaged, leading to corporate governance problems. For example, a user can employ FTP to send a large file, but there is no management of the data once the file has been sent. It can sit on an FTP server for many years, leading to potential data breaches from unauthorized parties outside a company, or unauthorized access to individuals inside the company.

GROWING STORAGE IN EMAIL IS A MAJOR PROBLEM

Many of the problems associated with managing email are directly related to its use as a file-transfer system. For example, an Osterman Research report[ii] published in September 2011 found that four of the top five problems in managing email systems are directly related to email's use as a file-transfer and storage system:

- Increasing backup and restore times (54% cite this as a serious or very serious problem)
- Increasing message size (48%)
- Lack of messaging-related disk space (40%)
- Mailboxes are overloaded (39%)

Because email storage is growing in excess of 20% annually, these problems will get significantly worse over time.

The result is that costs are driven up because more storage is being deployed in corporate email networks, more IT time is needed to manage email systems, and overall email system

performance degrades. It is important to note that the issue is not the cost of storage itself, since the cost of storage hardware is actually declining fairly dramatically over time. Instead, the issue of storage is the cost of IT deploying and managing it – this can be anywhere from five to eight times the cost of the storage solutions themselves.

FILE TRANSFER CONSUMES LOTS OF EFFORT

Managing file transfer is a relatively time-consuming effort for IT staff. If FTP systems are used, then IT must manage FTP servers and deal with user issues as they arise. If email is used instead of FTP or – more commonly – in addition to it, then IT must spend time dealing with email problems that are caused by the use of email as the file transfer backbone, as discussed above.

RELIABILITY AND SPEED OF FILE TRANSFER NEEDS IMPROVEMENT

One of the fundamental problems with FTP is its reliability. For example, FTP cannot inherently recover from an error, it does not send an alert when a problem has occurred, and it has problems with very large files in some situations. Moreover, FTP will often not maximize the available bandwidth, sending files at a maximum speed that is only a fraction of the available bandwidth. This not only means that transfers take much longer than necessary, but that the value of the purchased bandwidth is not being realized.

THERE ARE INADEQUATE MOBILE SOLUTIONS

Another problem with conventional file transfer solutions is that there are not a lot of good solutions for mobile users. While some cloud-based file transfer or file synchronization solutions offer good mobile capabilities, these consumer-focused often do not fit well in an enterprise environment because they do not allow IT to govern content as they should – the solutions work well for individuals, but not for the organization as a whole.

FINDING DATA IS NOT EASY

A serious problem with current file transfer capabilities is that they do not allow data to be found easily, if at all. For example, if users are employing any of the easy-to-use cloud-based file transfer or file synchronization solutions, they have addressed their personal requirements for file transfer. However, what happens when the organization needs to perform an early case assessment in advance of a legal action or a regulatory audit? What happens when they need to go through an e-discovery exercise or perform a legal hold? The dispersion of data across the various file transfer solutions that might be in use in an organization – and the inaccessibility of these data stores to IT or legal – can create serious problems for an organization when they need to find data in a timely manner, assuming that they can even access it at all.

CONTENT IS NORMALLY SENT UNENCRYPTED

The majority of emails and their attachments are sent by users without any encryption. This not only increases the potential for sensitive or confidential information to be exposed to

A dedicated and secure file transfer solution can make life much easier for the IT department in a number of ways, by reducing the reliance on email as the file transfer backbone, by allowing IT to manage corporate data in compliance with corporate policies, and by eliminating non-secure solutions that force IT staffers to scramble when e-discovery or other problems arise.

unauthorized parties, but it increases the risk of non-compliance with a growing variety of legal and regulatory obligations to protect sensitive data in transit. For example, 46 of the 50 US states now have data-breach notification laws, and two US states (Nevada and Massachusetts) have enacted statutes that require the encryption of certain content types when sent to individuals in those states. Content that is not encrypted can create enormous liabilities for an organization that suffers a data breach caused by unencrypted email being exposed or lost, even if the owners of that information do not suffer any harm as a result.

THE BOTTOM LINE: A DEDICATED, SECURE FILE TRANSFER SOLUTION IS NEEDED

The fundamental issue, then, is that organizations need a dedicated and secure file transfer solution to address two important issues:

- **To ease the burden on IT**
  A dedicated and secure file transfer solution can make life much easier for the IT department in a number of ways, by reducing the reliance on email as the file transfer backbone, by allowing IT to manage corporate data in compliance with corporate policies, and by eliminating non-secure solutions that force IT staffers to scramble when e-discovery or other problems arise.

- **To reduce corporate risk**
  More importantly, such a file transfer solution can substantially reduce corporate risk by putting all corporate data under the centralized management of the IT department, compliance department or some other authority within the organization instead of under the control of individual users. This can dramatically reduce the potential for data breaches, lost data, spoliation of data in legal actions, or an inability to meet regulatory or other corporate governance requirements.

Important Considerations in Selecting a Solution

The choice of a file transfer solution will be dependent on a number of factors, including the size of the organization, how distributed its employees are, the industry(ies) it serves, the regulations that it must satisfy, its corporate culture and other factors. However, there are a number of issues that decision makers should consider as they evaluate the best file-transfer solution for their organization:

- **Make it easy for users and align with existing processes**
  One of the most important considerations in selecting a managed file transfer solution is to integrate it as seamlessly as possible into the way that employees work today. A solution that requires a fundamentally different approach to file transfer, or that requires significant training for end users, simply won't be used and will be a wasted investment. The key is to deploy a solution that is as easy to use as consumer-oriented, cloud-based file-sharing options, but that do not create a paradigm shift.

- **Reduce (or at last don't add to) IT costs**
  Another important consideration is to use managed file transfer as a way of addressing the significant costs associated with IT having to manage existing storage and other problems

in email and FTP. Because the costs associated with storage-related problems in email systems can sap IT budgets, not to mention the costs associated with managing FTP servers and the like, a managed file transfer system can actually pay for itself in short order by reducing these costs. While a managed file transfer solution should be able to reduce storage and related costs, at a minimum the solution should not add to the IT department's budget requirements.

- **Allow the management of content throughout its life cycle**
  One of the fundamental benefits of a managed file transfer solution is its ability to manage content throughout its lifecycle. Unlike the case with most email and FTP systems in which content is largely unmanageable after it is sent, the right managed file transfer system will permit content to be managed by the senders and by IT with capabilities like making the content available only for a certain period of time or allowing its access only by authorized parties. This will make data breaches much less likely and will improve the ability to manage data in accordance with regulatory, legal and corporate policy requirements. Additionally, some solutions go beyond file transfer to offer file sharing, sync, commenting, and online workspaces for increased collaboration and productivity.

- **Satisfy current and anticipated corporate governance requirements**
  Corporate governance of data is becoming a much bigger issue as state, provincial and national governments are increasingly focused on data breaches and the consequences associated with them. Given that 2011 saw a number of major data breaches, we anticipate that laws and corporate policies focused on governing data will become stricter in 2012 and beyond. A robust managed file transfer solution will be able to satisfy current governance requirements – such as HIPAA, Sarbanes-Oxley and PCI DSS – and address future ones, as well.

- **Improve the performance over conventional file transfer**
  While most organizations will not frequently send multi-gigabit files, another important consideration in selecting a file transfer solution to replace FTP or other protocols will be to improve the speed of transfer. This improves the delivery time for very large files and makes better use of available bandwidth.

- **Allow anywhere, anytime, any device access**
  The ability to send and receive content using a managed file transfer solution should be universal, allowing users to send from any device and from any location. Consequently, a good managed file transfer solution will have a robust mobile capability that will support all of the smartphone and tablet platforms in use by an organization, as well as from more traditional venues like desktops, laptops and Web browsers.

- **Meet departmental and workgroup needs, not just individual needs**
  There are several good managed file transfer solutions that can satisfy individual requirements for sending large files independently of email. However, most organizations will

A good managed file transfer solution will have a robust mobile capability that will support all of the smartphone and tablet platforms in use by an organization, as well as from more traditional venues like desktops, laptops and Web browsers.

need a sharing and syncing solution that can satisfy the needs of departments and workgroups, as well as meet the needs of the overall organization, in order to satisfy the collaboration requirements of individuals and groups who must work together.

- **Provide granular file and folder access control**
  A robust managed file transfer solution will enable granular file and folder access control so that individual files and folders can have access rights or specific availability periods applied to them. Related to this is the need to apply appropriate security to content so that only those users who are authorized to access content can view or download files. Moreover, granular expiration periods need to be applied to certain types of data so that it is no longer available after a certain date or time.

- **Provide tamper proofing and audit trail capabilities**
  It is imperative that any managed file transfer solution prevent content from being modified. For example, a contract or proposal must be not be modified from the original unless the sender has authorized the changes. Moreover, a good managed file transfer system will provide robust auditing capabilities so that anyone who accesses content will be logged and their attempted changes captured. Both of these capabilities are critical to prevent charges of spoliation of evidence, and to apply appropriate governance to corporate content.

Summary

While email is universally deployed and has become the de facto file transport system for most users and most organizations, there are inherent problems with this method of sending content. Not least among the problems are the enormous strain placed upon email systems, the inability to appropriately govern content when sent through email, and the significant risks associated with data breaches and evidence spoliation.

To address these problems, every organization should deploy a managed file transfer solution. Doing so will reduce many of the storage-related and other problems associated with email systems, and will reduce overall corporate risk. The appropriate managed file transfer solution will provide granular control over content and minimize the impact on users' workflows and work patterns.

Sponsor of This White Paper

FileCatalyst, created by Unlimi-Tech Software, is a software platform designed to accelerate and manage file transfers. FileCatalyst is immune to the effects that latency and packet loss have on traditional file transfer methods like FTP, HTTP or CIFS. Global organizations use FileCatalyst to solve issues related to file transfer, including content distribution, file sharing and offsite backups.

The FileCatalyst transfer protocol is much faster than FTP, and is capable of reaching 10 Gbps speeds. Compare transfers for a 10GB file (more than two DVDs):

FileCatalyst®
reinventing file transfer

Unlimi-Tech Software, Inc.
Suite 205, 1725 St. Laurent Blvd.
Ottawa, ON
K1G 3V4
Canada

+1 613 667 2439
www.filecatalyst.com

Speed	Latency (ms)	FTP Transfer Time	FileCatalyst Transfer Time
100 Mbps	100	8 hr 18 min	14 min
10 Gbps	100	53 min	14 sec

FileCatalyst Webmail – built on the FileCatalyst platform – solves the problem of large file transfers by securely storing files on your own server while using email for communication. The process of sending a file is virtually identical to that of sending an email attachment, making adoption painless. Files sent with Webmail generate a transactional history that provides governance as well as audit information. Additional features include online storage boxes, user groups, LDAP/Active Directory integration and an Outlook plugin.

FileCatalyst Workflow, also built on the FileCatalyst platform, combines two powerful web-based managed file transfer workflows: submission and distribution. Users may submit files to your organization for processing, with full tracking at every stage; or they may securely distribute files to anybody with an email address. Additionally, one or more "file areas" allow users to store files in your organization's private cloud for online access from anywhere in the world.

[i] Source: *Results of a Survey on End User and IT Messaging Issues*; Osterman Research, Inc.; published April 2010

[ii] Source: *Content Archiving Market Trends, 2011-2014*; Osterman Research, Inc.; published September 2011