Evaluating Managed File Transfer in the Cloud: What You Need to Know

An Osterman Research White Paper

Published October 2012

SPONSORED BY

IPSWITCH
FILE TRANSFER

OSTERMANRESEARCH

EXECUTIVE SUMMARY

Every organization needs to have a secure and reliable method to manage, govern and automate their file exchange processes. After all, an uncoordinated approach puts the security and availability of critical data at risk.

A file exchange strategy has multiple components to it. Most organizations are facing challenges with person-to-person file exchange, and along with this we see the B2B, system-to-system, and system-to-person aspects of file exchange are growing in importance and are increasingly subject to security and other concerns.

Although most organizations today use email, FTP, scripting, cloud-based document repositories and other tools to send files, these modes of file transport suffer from a number of problems, including a lack of auditability of the sent files, a lack of reporting capabilities, no visibility into the transfer process, and an inability to enforce access or permission controls over the content. To overcome these problems, organizations must be able to:

- Enforce IT, security and compliance policies across the entire organization for every kind of file transfer.

- Automate data transfer processes and workflows so as to improve their efficiency.

- Replace old and insecure scripts that can lead to policy violations.

- Enable straightforward person-to-person file transfer.

In short, traditional tools and processes used for file transport typically do not provide the necessary level of control over content and access, resulting in a much higher likelihood of a data breach, inefficient or slow delivery of content, and reduced employee productivity.

SO WHAT?

Organizations require a managed file transfer solution that will overcome the problems with current processes and workflows: one that will enable organizations to manage and govern the exchange of files and data. Such a solution needs to enable full administrative control over how and where content is sent, who has access rights to the sent files, full encryption of the content throughout its lifecycle, and the ability to reduce data risks and drive the costs of file transfer as low as possible.

Organizations of every size should seriously consider adopting a cloud-based managed file transfer solution to compliment, or potentially replace, an on-premise file transfer solution. The advantages of managing file transfer in the cloud and include:

- Virtually no up-front costs
- More predictable costs over the life of the system
- Rapid deployment
- Conservation and refocus of in-house IT resources
- Guaranteed uptime
- Greater scalability and flexibility
- Robust security
- Built-in disaster recovery
- The ability to integrate with an on-premise managed file transfer solution

A cloud-based file transfer solution integrated with on-premise capabilities can be useful for geographically distributed organizations, allowing field offices without dedicated IT staff to have the same level of functionality as a headquarters served with an on-premise solution.

Organizations require a managed file transfer solution that will overcome the problems with current processes and workflows: one that will enable organizations to manage and govern the exchange of files and data.

ABOUT THIS WHITE PAPER

This white paper discusses the critical role of managed file transfer, why a cloud-based managed file transfer service is a viable alternative or compliment to on-premise solutions, and key issues to consider when evaluating various cloud offerings.

WHY MANAGE YOUR FILE TRANSFER OPERATIONS?

The transfer of files between systems and applications behind a corporate firewall, between internal systems and those of business partners, or between users is an essential part of the communications flow for any organization. Given that the vast majority of the bits that flow through corporate networks are files, there are four reasons that every organization must manage its file transfers properly:

1. **To improve corporate governance**
    Corporate governance over information transfer is absolutely essential and is becoming more important as a result of increased oversight by government. Statutory and other requirements – such as HIPAA, Sarbanes-Oxley, PCI DSS, Basel II and the Gramm-Leach-Bliley Act – require that organizations manage information transfers properly. Specifically, a sound file transfer process should provide for the following elements:

    o   Administrative control so that IT or another corporate entity can manage the flow of information in a company

    o   Compliance auditing and reporting to ensure that information is sent in accordance with corporate policies and legal requirements

    o   Visibility into the file transfer process so that, as discussed in the point above, the transfer of files can be tracked and audited through the information lifecycle

    o   Highly secure file transfer processes in order to minimize the potential for a data breach, and also to enable control of the information and for how long it can be accessed

    o   Fundamentally, corporate governance is about reducing corporate risk – any file transfer system must minimize the risk of data breaches or other problems to the greatest extent possible

2. **To improve corporate processes and workflows**
    Another important reason to implement a secure managed file transfer solution is to improve the management and efficiency of data transfer workflow processes. Using a robust managed file transfer solution can replace scripting processes – which are often complex, hard to maintain and insecure – and allow for the automation of workflows in an organization. This can make workflows more reliable, as well as improving the compliance and governance capabilities over these work processes. Moreover, a robust MFT solution can increase productivity by automating manual and labor-intensive processes; simplify the creation of complex, multi-step and logical workflows; run processes on a schedule-driven, event-driven or on-demand basis; and integrate with third-party schedulers, scripts and applications to control workflows.

3. **To provide secure, reliable and guaranteed delivery for all types of file and data transfer**
    Appropriate management of file transfers between applications or individuals is essential in order to enable secure and reliable transfer of critical information. MFT lets an organization enforce IT, security and compliance policies

Using a robust managed file transfer solution can replace scripting processes – which are often complex, hard to maintain and insecure – and allow for the automation of workflows in an organization.

consistently; provides reporting and analysis to measure performance and ensure that SLAs are met; and allows business-to-business, multiprotocol connectivity. In the absence of MFT:

- o   Content is not encrypted in most cases.
- o   There is no proof that the content has actually been received.
- o   Content cannot be tracked after it is sent.
- o   There is no control over how long the sent content is available for access.
- o   Access permissions cannot be established for content that is sent.
- o   There is no audit trail for the delivery of information.

In short, without a sound file transfer mechanism in place, there is little control or visibility into the file transfer process.

4.   To alleviate the burden on email systems
Another important reason to implement a sound managed file transfer solution is to alleviate the enormous burden on email systems. Today, the vast majority of files that are sent person-to-person use the email backbone to provide transport for this content. The result is that more than 95% of the bits that flow through email systems today are files and not email messages themselves.

The consequences of using email as the file transfer system are several and include higher IT costs to manage the rapidly growing storage requirements in most email systems, wasted user time cleaning out mailboxes in order to stay under mailbox size quotas, slower message delivery, increased email server downtime, longer nightly backups, and longer restores after an email server crashes. Using a true file transfer system that employs an email client plug-in or a browser-based interface will result in faster email delivery, greater email server reliability and lower storage costs.

WHY MANAGE YOUR FILE TRANSFER OPERATIONS IN THE CLOUD?

Clearly, managing and governing file transfer operations is essential to improving corporate workflow processes, ensuring the reliability of information delivery, and mitigating risk. While managed file transfer systems can be deployed on-premise or in the cloud, there are several key reasons to consider for managing file transfers using cloud services:

- •   **Virtually zero up-front cost**
  Unlike on-premise managed file transfer systems that require the purchase of servers and software, there are virtually no up-front costs associated with a cloud-based managed file transfer capability. The switch from a capital expenditure (CAPEX) model to an operating expense (OPEX) model is one of the most compelling reasons for switching to a cloud-based service, since IT does not have to devote a significant portion of their available funds to the deployment effort in a single budget cycle.

- •   **Predictable ongoing costs**
  Related to the near zero up-front cost of a cloud-based managed file transfer service is that ongoing costs are predictable over the life of the service provider contract. Unlike on-premise systems that may require unexpected IT attention when things go awry, cloud services offer a predictable cost per user over a long period. Even as users are added to the system because of company expansion, the cost of the managed file transfer service will increase predictably and steadily.

- •   **Use of in-house IT labor for more productive work**
  For the vast majority of organizations, managing a file transfer capability cannot be considered a core competency. The result is that even if an on-premise

Unlike on-premise managed file transfer systems that require the purchase of servers and software, there are virtually no up-front costs associated with a cloud-based managed file transfer capability.

managed file transfer system is managed extremely well, IT's management of it – no matter how important file transfer is to the organization – will not add significant value to the organization by virtue of internal IT staff managing it.

However, if IT does not have to deploy or maintain an on-premises MFT capability, this will save time and money, plus increase IT staff members' availability to focus on other key initiatives. A cloud service would free up IT resources that would otherwise be responsible for deploying, managing and maintaining complex partner, applications and collaborative file and data transfers, since internal IT staff would not have to deal with software installs, hardware maintenance, patching and other activities necessary to maintain on-premises infrastructure.

- ***Deployment in hours, not weeks or months***
  Another important advantage of a cloud-based managed file transfer capability is that it can be deployed very rapidly – typically within a few hours – unlike on-premise systems that can take weeks or months for the purchase of servers and software, their deployment and configuration, and their integration with other on-premise systems. All a company needs to do is provision its users and the service can be used almost immediately.

- ***Built-in high availability***
  Typically, cloud-based managed file transfer capabilities offer very high levels of reliability. Of course, this is dependent on the provider selected, but most leading providers have deployed a carrier-grade infrastructure that includes redundant communication links between multiple data centers, replication of customer data between these data centers, backup generators, and 24x7 staffing. For most organizations, the cost and expertise to reproduce this level of reliability using on-premise systems would be prohibitive.

  While on-premise managed file transfer systems can be highly reliable, cloud-based services are generally more reliable. For example, if an on-premise managed file transfer system experiences just four hours of downtime per month for activities like server upgrades, maintenance and other planned activities, this will result in a maximum annual uptime of 99.45%. Add in unplanned events like power outages or server crashes totaling another hour of downtime per month, and the uptime figure drops to 99.32%. While this level of uptime is reasonable for most on-premise systems, leading cloud-based providers generally provide 99.9% uptime.

- **Can extend the investment in on-premise MFT to the cloud in a hybrid architecture**
  A managed file transfer capability need not be an on-premise or cloud decision: many organizations are taking a hybrid approach by deploying both. For example:

  o An organization can maintain revenue-driven B2B and B2C transfers – such as purchase orders, shipping, inventory, etc. – on-premises and move other types of file transfers to the cloud.

  o Critical customer and partner data transfers could be kept on-premises to provide the highest levels of support, while less time-sensitive or less critical transfers could employ a cloud service.

  o An organization could opt to create and schedule multi-step transfer workflows and processes on-premises, but then have them executed in the cloud to save on-premises IT resources, cost and bandwidth.

  o Highly sensitive data that is subject to strict regulatory control, such as customer financial information, could be transferred using on-premises capabilities, while less sensitive data could be transferred using a cloud

Another important advantage of a cloud-based managed file transfer capability is that it can be deployed very rapidly – typically within a few hours.

service. Conversely, a company that is not confident in its internal ability to meet strict regulatory obligations could use a reliable cloud provider for its most sensitive transfer operations, and use internal capabilities for less sensitive transfers.

- **The right cloud provider will offer a robust and secure infrastructure**
It is absolutely essential that any provider of cloud-based managed file transfer services offer a highly reliable infrastructure that can handle the load placed on its by its customers. However, just as important is the fact that the infrastructure be highly secure so that breaches of data cannot occur. This requires the cloud provider to deploy robust physical security for any location that houses customer data, as well as robust security and encryption against malware, hackers, advanced persistent threats and the like. Because even a single data breach can cost multiple millions of dollars to remediate, security for a cloud-based provider of managed file transfer capabilities must be bulletproof. Cloud providers that properly manage their customers' data will not permit their unauthorized users to access any customer content.

- **More scalable and elastic than on-premise deployments**
Another important advantage of a cloud-based managed file transfer capability is that it is more easily scalable and elastic than on-premise deployments. In other words, a cloud service is better able than on-premise systems to scale upward to meet spikes in usage, as well as to scale down to reduce costs when demand slows. The latter is particularly important for companies that are seeking to reduce costs after a reduction-in-force or during a seasonal slowdown of file transfer activity. When managed on-premises, additional software licenses, additional hardware or additional bandwidth may need to be deployed just in case spikes in demand necessitate it – this is not the case with cloud providers that already have excess capacity and can simply deliver more bandwidth on demand.

- **Built-in disaster recovery**
Another advantage of a cloud-based managed file transfer system is that – with the right provider – disaster recovery is built-in. This is particularly important for organizations that have gone through some sort of natural disaster or other unforeseen event that could prevent them from accessing their on-premise infrastructure. The use of a cloud service for file transfers will enable employees to continue working even when their primary office location is unavailable.

KEY ISSUES TO CONSIDER WHEN EVALUATING SERVICE OFFERINGS

When evaluating cloud-based managed file transfer offerings, there are four important issues that should be considered:

- **There are wide variations between cloud service offerings**
There are two basic classes of offerings that often get lumped together as "managed file transfer" offerings. The first are true MFT solutions that provide visibility of files and data throughout the entire transfer process and its lifecycle; enforcement of IT, security and compliance policies consistently, such as access control; auditing and end-to-end encryption of files. The second group of offerings are basic storage and synchronization services that will enable collaboration between employees, suppliers and customers. Moreover, using a platform-as-a-service offering based on an offering like Amazon's EC2 on which another vendor's solution is deployed still requires multiple points of contact to resolve problems, perform upgrades, etc.

It is important to note that both classes of solutions are useful and can be complimentary, but they are used for fundamentally different purposes. Solutions in the first group are designed for highly secure, highly auditable file

A company that is not confident in its internal ability to meet strict regulatory obligations could use a reliable cloud provider for its most sensitive transfer operations, and use internal capabilities for less sensitive transfers.

transfer processes that enable a high degree of corporate governance. Solutions in the second group are designed solely for sharing files between individuals or helping individuals or workgroups to keep a set of files synchronized across multiple platforms. Again, both classes of file transfer products are useful, but they are not interchangeable.

- **Price is important, but should not be the primary consideration**
  Another important consideration for any cloud-based managed file transfer solution is its price. There is variability between the prices for different offerings, but price should typically not be the primary consideration when it comes to solutions that are so integral to a company's processes. Moreover, given the enormous cost of even a single data breach, the security and governance capabilities of the solution should be considered as more important than the price of the solution itself.

- **Consider all of the costs associated with on-premise file transfer**
  When comparing the costs of an on-premise managed file transfer solution versus a cloud-based alternative, it is important to factor in all of the costs of the former. Our research has found that many decision makers do not add in all of the on-premise costs when making the comparison, giving on-premise solutions an unfair cost advantage in the analysis. For example, all of the following costs should be factored into the cost of an on-premise managed file transfer solution:

  o Physical infrastructure, such as server hardware, operating systems software, application software and other capabilities. Given that the deployment of an on-premise solution requires a significant amount of up-front capital expenditure, it is important to account for all of the infrastructure elements that are required to maintain the on-premise managed file transfer system.

  o The IT labor that goes into evaluating, configuring, deploying, maintaining and upgrading the on-premise infrastructure.

  o The financial and possible tax benefits of migrating from a capital expenditure (CAPEX) to an operating expense (OPEX) model. This can create significant financial benefits for an IT department that does not have to budget for large expenditures to deploy hardware and software and the IT labor that goes along with deployment.

  o Power costs, which can add substantially to the cost of an on-premise solution. For example, assuming that a managed file transfer server consumes 750 watt-hours of electricity during normal operation, the annual cost to operate this server will be $1,084 per year[1] in Connecticut where electricity prices are fairly high. Even in Idaho, where electricity costs are low, the annual cost to run this server will be $445 per year[2].

  o Heating, ventilation and air conditioning costs for the on-premise equipment.

  o The cost of floor and rack space to house the servers.

  o The opportunity cost of the IT labor devoted to managing the solution.

  The last cost element is one that many organizations overlook because they consider it to be a "sunk" cost of an on-premise system. For example, if we assume that an IT staff person must spend four hours per week overseeing the on-premise managed file transfer infrastructure, and that the fully burdened cost of that IT staff person is $80,000 annually, the annual cost to manage the system will be $8,000. However, while this cost is significant, the cost of not

When comparing the costs of an on-premise managed file transfer solution versus a cloud-based alternative, it is important to factor in all of the costs.

---

[1] http://www.electricchoice.com/electricity-prices-by-state.php
[2] Ibid

using this individual for a project or initiative that could yield more value must also be factored into the equation. Given that good IT staff people are not particularly easy to find, using part of an individual's time to oversee a managed file transfer system could be a waste of a valuable and scarce IT resource.

- **Compare the security of on-premise and cloud-based file transfer offerings**
  Finally, it is critical to accurately compare the security of on-premise and cloud-based managed file transfer solutions. While many decision makers are reluctant to consider the latter because of their fear that sensitive or confidential data will be compromised when in the hands of a third party, it is important for these decision makers to ask themselves the following questions:

  o How secure are the rooms in which managed file transfer servers are currently housed in our company?

  o Do these rooms require two-factor authentication to enter as is the case with leading cloud providers?

  o Is a log kept of all visitors who access these rooms?

  o Are we absolutely certain that unauthorized parties will not be able to gain access, such as might occur if an employee holds open a door for a visitor?

  o Do our physical facilities comply with standards and practices like PCI, FIPS-140, SSAE 16 Type II SOC 1 or Safe Harbor?

  o Do our administrators have access to the data files?

  o Can we provide a complete audit trail of all activities that occur in our on-premise data center?

  o Do we provide for granular access controls and enforce strict user permissions for all content stored in our on-premise data center?

  o How robust are our internal intrusion detection and intrusion prevention systems?

  o Do we provide end-to-end encryption for all data, both in-transit and at rest?

  o What does it or will it cost to maintain such tight controls using only on-premise systems and in-house IT personnel?

  In short, a thorough comparison of on-premise versus cloud-based managed file transfer systems will most often result in the nod going to the latter.

Decision makers should seriously consider using a cloud-based managed file transfer solution in order to reduce the total cost of ownership for this capability relative to an on-premise solution.

SUMMARY

A managed file transfer solution is essential for any organization to transfer content between individuals and systems. Such a solution should provide highly secure transfer of content, auditing capabilities, maintenance of strict compliance with corporate and other policies, be as inexpensive as possible to operate, and operate independently of the corporate email system. Decision makers should seriously consider using a cloud-based managed file transfer solution in order to reduce the total cost of ownership for this capability relative to an on-premise solution, and to maintain highly secure transfer capabilities.

ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer is a global provider of managed file transfer solutions that deliver the control necessary to enable governance and compliance with the ease-of-use that supports broad end-user adoption. Millions of global users - including the majority of Fortune 1000 enterprises and government agencies rely on Ipswitch for their file transfer needs and data workflow needs, with solutions both on-premise and in the cloud.

Learn more at http://www.ipswitchft.com.