3 Top File Transfer Challenges for Financial Services IT Teams

ipswitch

ipswitch

Introduction

Financial Services organizations should pay particular attention to the use of unsecured file share technologies such as email, unencrypted FTP and consumer-grade cloud services by employees and external partners

Just like in other financial services organizations, your IT team continuously strives to improve your ability to deliver non-stop, high performance services in support of the business. It can be surprising how big a role file transfer services can play in that effort. This paper will examine the three specific and unique challenges faced by financial services IT teams like yours, and the file transfer capabilities you will need to address them.

Financial services firms transfer huge amounts of data every day. Too many IT teams supporting these transfers are wasting valuable resources in manual scripting and management efforts. By consolidating disparate file transfer processes while migrating to a centralized system, you can achieve improved reliability and security while reducing IT workloads and costs.

A Critical Business Process

"File transfer" is a broad term that impacts many layers of an organization. It may involve transferring data internally, between your own systems and processes. It may include transferring data between your systems and those of outside business partners. In some cases, it may involve the ad-hoc transfer of data between individual users or systems. In an increasing number of enterprises, these file transfers have become numerous enough and complicated enough to require new tools that are better suited for core business processes.

Historically, many financial services organizations have taken a do-it-yourself (DIY) approach to file transfer. These likely started with legacy FTP operations and scripts that were built to provide some level of automation for often repeated transfers.

However, as file transfers become core business processes with the concurrent need to protect data in transit, these DIY approaches prove problematic. In few industries is this more true than in the financial services realm, where security is paramount, and where unique business drivers quickly make DIY techniques not only undesirable but completely unacceptable.

ipswitch

The Top 3 Challenges Facing Financial Services IT Teams

While challenges like security and operational stability are not unique to the financial services industry, this unique business environment creates unusual technical requirements and concerns that aren't often observed elsewhere.

Reliability and Performance

Financial services firms have astonishingly little room for error. They deal in incredible volumes of data, must process that data in extremely short time windows and must be 100% accurate in every operation they undertake. Financial services customers expect companies to be available 24 x 7 x 365, meaning every service simply must be on-line and working all the time.

Home-grown FTP and script approaches fall short of these business requirements. Consider custom-scripted solutions, for example, which range from simplistic FTP scripts to elaborate, multi-step scripts written in a variety of programming languages. These tend to be inefficient when dealing with the volume of tasks that financial services firms must transfer, simply because these scripting languages were never designed for that level of performance.

Scripted solutions are difficult to make highly-available. These solutions are also costly to maintain, usually requiring specialized on-staff expertise to support critical business processes. An enormous amount of time and money can be required to make custom-scripted solutions reliable, as their programmers must be prepared for a variety of failure situations that often can't be anticipated in advance.

Performance is hyper-critical in a financial services organization. Transactions must be completed quickly to meet customer expectations. For example, when a customer wants to transfer rewards points from a credit card to a partner airline, they want that transaction to occur as close to instantly as possible.

These shrinking processing windows create challenges for custom-scripted FTP solutions, as well as for low-end off-the-shelf software packages and cloud-based, consumer grade file sharing services.

ipswitch

Security and Compliance

It's obvious that the data transmitted in financial services file transfers can be extremely sensitive. Government and industry data protection regulations place an enormous burden of responsibility on financial services firms to secure that data from theft or misuse. That responsibility creates a cascade of technological and business requirements.

One of those is a need for the absolute best encryption technologies, including government-certified encryption modules that protect data not only while it is being transmitted, but also while it sits "at rest" on whatever systems or servers that are processing it. Authentication is also crucial, with a need for stronger and more reliable authentication mechanisms than simple user names and passwords – such as strong, multi-factor authentication.

Visibility is another strong requirement. It isn't enough to simply be compliant with the rules and regulations affecting your firm, you must also be able to demonstrate that compliance through detailed audit logs and record keeping. That means generating audit entries each time a piece of data is touched, moved, accessed, or manipulated in any way. Even a fully-compliant firm faces enormous penalties for failing to demonstrate that compliance through acceptable audit logs.

Manageability and governance are also key drivers. Firms are continually seeking to improve their bottom line by reducing their overhead, and to manage their IT systems according to industry and regulatory best practices and requirements.

If your IT team is attempting to meet these security, auditing, and manageability requirements using low-end or custom-scripted solutions, it is likely costing you more in IT staff productivity losses than you are saving it systems costs. Those solutions were simply never designed with these requirements in mind.

You can't, for example, simply tack on auditing to an FTP script. You can't run out and buy encryption software that integrates tightly enough with a low-end solution to provide truly end-to-end protection for your data. These requirements can't be met through patches, add-ons, or in a piecemeal fashion. They must be an integral part of a complete solution.

ipswitch

Better Services - Reduced Costs

A financial services business depends on its ability to continuously improve services to compete. Especially today, customers have an expectation of modernity and convenience that can dictate their choice of who they want to do business with. This expectation also extends how you enable your business customers to extend new services to their customers.

A great example of this is the convenience of a highly automated mortgage processing system. Brokers and lawyers that deal in mortgage processing are competing for customers on a word of mouth basis. If your business systems require manual processing of approval forms the resulting inconvenience to end customers will cause you to lose mind share to better automated competition.

Just imagine which experience you would recommend. Your mortgage approval process involves manual workflows and entails a one day turn around from application to approval. Your competitors mortgage approval process is highly automated. Incoming applications are electronically passed to an available loan processing agent. The mortgage applicant gets an approval in the time it takes to enjoy a cup of coffee in the lawyers office and discuss the weather. Your business success depends on your ability to compete effectively and today that translates to technology implementations.

You can also imagine the IT workloads that result from outdated scripts that cause delays, missing files or may not even be compliant. Contrast that workload with those resulting from automated workflows that minimize human error and that document file transfer activities and user access to sensitive data in support of your next audit.

It is likely that years of past efforts to meet a varied set of needs for file transfer may have resulted in a great deal of overlap, repeated effort and redundancy in your file transfer processes. Redundancy of this kind invariably equals increased cost and risk, and firms are justifiably trying to reduce both. Consolidating redundant functionality into centralized, easier-to-support, more consistently-manageable solutions can pay huge dividends in reducing IT workloads and operating costs.

Such a system could be maintained by a central IT team and offered as a service to the firm's various divisions, enabling each division to continue managing its own resources, but to do so in a way that is consistent with top-down policies and requirements.

Secure Managed File Transfer

When an organization's file transfer needs for reliability, manageability and security out-grow their home-grown FTP legacy systems, Secure Managed File Transfer present an ideal evolution.

Below are some of the key features that form the rational for IT teams to migrate to Secure Managed File Transfer. We also provided notes on how Ipswitch's MOVEit delivers these capabilities.

Automation

Automating file transfer operations has multiple benefits. It cuts down on the likelihood of lost revenue from late SLA submissions. It also reduces the risk of violating security requirements required to comply with data protection regulations.

The automation of file-based tasks and business workflows enables IT to:

- Minimize the need to maintain multiple scripts
- Meet service line agreements (SLAs) requirements
- Stay flexible in order to adapt to changing business conditions
- Eliminate the need to manually monitor where files are at any given time.

MOVEit Automation supports guaranteed delivery via automatic forwarding and error correction capabilities for all data transfers that take place. Delivery assurance is achieved by automatically resubmitting a failed file transfer activity until it completes successfully. Once the data is delivered, MOVEit provides the sender with a notification confirming that the data was received by the authorized recipient(s).

Visibility and Control

Control as to who accesses or transfers data and visibility over its movement can greatly minimize the risk that hackers gain unauthorized access to sensitive data. By having clear insight into data flows and events taking place, your organization will be able to put effective security procedures in place to protect your data and help assure compliance with data protection compliance regulations.

MOVEit provides a large set of authentication controls manage when and for how long users are authorized to access sensitive data. Control over logging and reporting simplifies the audit process and assures the integrity of audit trails.

Information Security

Important file transfer compliance requirements include file integrity checks, data deletion after receipt, non-repudiation and guaranteed delivery. These information security safeguards ensure sensitive data in transit is protected from being altered by a third party or incorrectly delivered to an unintended recipient.

MOVEit's non-repudiation data integrity feature ensures that the sender and the receiver are both authorized and authenticated to access the data. In other words, only the sender and receiver have permissions to access the data that is being transmitted. If a third party somehow manages to intercept this transmission, they will not be able to read or alter any of the data.

Cryptography

Compliance standards often mandate a certain level of data security protocols be put in place to prevent sensitive information from ending up in the wrong hands, stolen and sold on the black market.

MOVEit uses FIPS 140-2 validated algorithms such as AES-256 encryption to protect data at rest. Even if someone is able to hack into your system, any data stored on the MOVEit Transfer server will be encrypted and inaccessible to the intruder. They will not be able to 'break the code', so to speak, and gain access to your sensitive files.

MOVEit also protects data in transit using secure file transfer protocols SFTP (SSH), FTPS (SSL/TLS) and HTTPS (SSL). These protocols are continuously updated in MOVEit to adhere to the latest industry standards, ensuring your data is always safe.

Failover

Business continuity is a very important aspect for any organization that must exchange sensitive data, both within and outside the confines of its firewall. You need to ensure that data in motion does not get "lost in a void" during a natural disaster, power outage or period of high transfer volume.

MOVEit's flexible and scalable architecture enables high availability by improving the network's file transfer performance. Failover can be gained by eliminating single points of failure with the implementation of a distributed web farm deployment of MOVEit Transfer components.

Ipswitch MOVEit

MOVEit provides reliable and secure file transfers of business critical data. It lets you manage, view and control all file transfer through a single system with the ability to:

- Manage all file transfer activity from a central location
- Transfer sensitive business files reliably and securely
- Automate file-based business processes
- Meet security and compliance requirements

MOVEit Transfer

Securely exchange files between partners, customers, systems and users.

MOVEit Automation

Easily develop simple to complex workflows without advanced programming skills.

MOVEit Cloud

The full functionality of MOVEit™ with the convenience of cloud-based deployment .

Ipswitch Analytics

Streamline compliance audit preparation and SLA reporting.

Ipswitch Gateway

Ensure the security of file transfer activities.

About Ipswitch

For today's hard-working IT teams relied upon to manage increasing complexity, Ipswitch IT and network management software delivers secure control of business transactions, applications and infrastructure. Our network and infrastructure monitoring software provides end-to-end insight, is extremely flexible and is simple to deploy. The company's Information Security and Managed File Transfer solutions enable secure, automated and compliant business transactions and file transfers for millions of users. Designed to be easy to try, buy and use, our simply powerful software helps teams shine by delivering 24/7 performance across cloud, virtual and network environments.

Visit our Website **Speak to a Specialist** **Request a Trial**