COVIANT Software

WHITE PAPER

SIMPLIFYING SECURE FILE TRANSFER:

Selecting a Best-In-Class Managed File Transfer Solution

EXECUTIVE SUMMARY

"Organizations must seek a scalable, secure, file-transfer infrastructure as a core solution to reduce complexity and speed deployment of Internet-based business processes."

– META Group

Corporations share data with a variety of remote offices, trading partners, customers, and regulatory agencies. Sensitive data – such as payroll information, human resources benefits, and corporate financials – is transferred to and from entities around the world billions of times a day. Security breaches are frequently in the news, with many reports of lost or compromised customer data. However, workflow breakdowns are more likely to occur and potentially just as harmful.

FTP or secure FTP is often the technology used to handle these transfers, where 'secure' refers to protecting data in transit. Most companies have FTP or secure FTP solutions in place today. While these technologies enable good point-to-point delivery of files, they are no longer sufficient to support the growing number of business processes that rely on electronic file transfers. As the volume of file transfers grows, managing these file transfers has become a critical business issue.

Today, it is common for organizations to use one product to handle data encryption, another for file transfer, and yet more products to meet workflow requirements – relying on custom programming to cobble together a viable solution. This practice is resource-draining and inefficient, given that corporations perform dozens or even hundreds of file transfers a day. According to 58% of respondents in a recent Information Week/Accenture Global Information Security Survey, "managing the complexity of security" is the biggest security challenge facing their industry.

A best-in-class Managed File Transfer solution must successfully address three requirements:

- Integration of data encryption, robust secure file transfer, and workflow management
- Compatibility with both your IT infrastructure and the IT infrastructures of your partners (i.e., open interoperability)
- Scalability to handle additional trading partners and higher file transfer volumes

As businesses require open interoperability and scalability, the term 'secure file transfer' does not adequately describe their file transfer management needs. While many products deliver some Managed File Transfer features, few products meet corporations' emerging requirements for a scalable, open solution.

Coviant Software defines a Managed File Transfer solution as an open, scalable product suite that integrates secure file transfer with workflow management.

1 | BACKGROUND

Managed File Transfer solutions contain four components:

1) Open interoperability provides the foundation of a successful and long-lived Managed File Transfer implementation, leveraging existing technologies and building upon standards compliance and vendor neutrality.

2) Workflow management is the wrapper around secure file transfer. Your organization's need for real-time event notifications, comprehensive audit capabilities, job monitoring, and rapid containment/recovery are all critical elements of the workflow management surrounding secure file transfers.

3) Secure file transfer is at the heart of a Managed File Transfer solution. Aspects to consider include end-to-end data protection, 24x7 automation, and in-process error correction.

4) Scalability is a combination of performance, maintenance, and re-use. You can expect the number of service providers, trading partners, and automated business processes that you use to increase over time, making scalability a key requirement for any Managed File Transfer solution.

This white paper concludes with a chart that you can use to compare features of Managed File Transfer products.

While data remains the lifeblood of business, it no longer courses solely within corporate boundaries. Today corporations share data with a variety of service providers, trading partners, customers, and regulatory agencies. Sensitive data – such as payroll information, human resources benefits, and corporate financials – is transferred to and from entities around the world billions of times a day.

FTP or secure FTP is often the technology used to handle these transfers, where 'secure' refers to protecting data in transit. Most companies have FTP or secure FTP solutions in place today. While these technologies enable good point-to-point delivery of files, they are no longer sufficient to support the growing number of business processes that rely on electronic file transfers. As the volume of file transfers grows, managing these transfers has become a critical business issue. Gartner Group states that file transfer management solutions need to "address the workflow considerations surrounding data transfers, over and above the security of the transfer itself."

A file transfer must integrate smoothly with the workflow of which it is a part. Security breaches are frequently in the news, with many reports of lost or compromised customer data. However, workflow breakdowns are more likely to occur and potentially just as harmful.

Here's an example. Your company sends payroll data to your bank every week, and you have set up a workflow process where the files are encrypted and sent to the bank's FTP server. However, this week the transfer fails, because logins have been temporarily disabled on the bank's FTP server.

The problem you have on your hands at this point is not a security breach. It's a business workflow issue, one that – if you aren't notified or don't have the capability to remedy quickly – has the potential for major impact on your business.

Secure file transfer and workflow management are intertwined in the real world; both must be addressed in order to have a comprehensive Managed File Transfer (MFT) solution. Because Managed File Transfer solutions are evolving, it's not easy to select the right product. Many vendors claim to offer MFT when their products don't go beyond basic secure file transfer functionality – there's no workflow integration. Other vendors support some workflow tasks, but lack features that have become essential. (See Section 4 for a checklist of these features.)

This white paper explores the current requirements for a best-in-class Managed File Transfer solution that delivers secure file transfer plus supports your workflow processes.

"Secure file transfer products in the past focused on secure communications.... But we need to start talking about automation and management." — Gartner Group

2 | Evolution of Secure File Transfer

The need for secure file transfer has accelerated as corporations control costs by conducting business over the Internet. File transfer using the Internet has replaced many traditional methods of sharing sensitive data with trading partners or remote offices, such as bonded courier services or private WANs. Unfortunately, the Internet is far from perfect when it comes to secure file transfer.

The Internet's popular file transfer protocol, FTP, is widely used but lacks the security features required today. FTP security can be enhanced by using SFTP (SSH) or FTPS (SSL) during the transfers to protect both login data and transaction file content, but another critical consideration in secure file transfer is "data-at-rest."

Files on systems outside of corporate firewalls must rely on encryption for protection. Standards-based encryption technologies, such as OpenPGP, have become popular. Secure file transfer products built on standards such as FTP and OpenPGP provide more flexibility as they lower the cost of technology.

Companies that use secure FTP plus file encryption probably have an adequate secure file transfer solution. However, they are likely missing a key component of a Managed File Transfer solution – incorporation of workflow management. FTP provides virtually no workflow support, having no inherent capability to automate file transfer, provide notifications, capture audit data, or assist in troubleshooting – all workflow requirements that we look at more closely in this paper.

Today, it is common for corporations to use one product to handle data encryption, another for file transfer, and yet more products to address workflow requirements. For the most part, IT organizations rely on custom programming to cobble these products together to deliver adequate functionality to the organization. But as the use of secure file transfers continues to escalate, manual approaches and custom programming are becoming too resource-intensive, difficult to manage, and prone to breakdown. Current file transfer practices are often a frustratingly inefficient and resource-draining approach to a straightforward set of operations that a corporation must perform dozens or even hundreds of times a day.

No wonder 58% of all respondents said that "managing the complexity of security" was the biggest security challenge facing their industry a recent Information Week/Accenture Global Information Security Survey.

Today, it is common for corporations to use one product to handle data encryption, another for file transfer, and yet more products to address workflow requirements.

3 | Evaluating Best-in-class Managed File Transfer Solutions

A best-in-class Managed File Transfer (MFT) solution needs to address all of the business and technical requirements in a single product, which means successfully addressing three requirements:

- Integration of data encryption, robust secure file transfer, and workflow management into a solution that makes it easy for IT staffs to automate, manage and troubleshoot the file transfer process. Gartner and others have identified these elements as core components of Managed File Transfer solutions.

- Compatibility with both your IT infrastructure and the IT infrastructures of your partners. Many older solutions, which require you and your service providers or trading partners to invest in proprietary products, are becoming less acceptable. Unless you have a strong influence over your partners' IT investments, a standards-based, vendor-neutral solution that delivers "open interoperability" is likely to be the preferred alternative.

- Scalability to deliver and manage substantial increases in file transfer volumes. As your file transfer environment expands, your MFT solution must deliver "scalability" by continuing to deliver excellent performance, manage relationships with an increasing number of trading partners, and keep up with maintenance tasks that may increase even more rapidly.

As businesses require open interoperability and scalability, the term secure file transfer does not adequately describe file transfer management needs. While many products deliver some Managed File Transfer features, few products meet corporations' emerging requirements for a scalable, open solution. Managed File Transfer solutions address secure file transfers and the surrounding workflow management – while offering easy interoperability with partners and the ability to scale as your file transfer needs expand.

Managed File Transfer Solution

Managed File Transfer solutions treat each file transfer as an integrated business transaction, not a set of technology tasks. A best-in-class Managed File Transfer solution must addresses the four essential elements of Managed File Transfer:

01 Open Interoperability

02 Workflow Management

03 Secure File Transfer

04 Scalability

3.1 Open Interoperability

Open interoperability provides the foundation of a successful and long-lived Managed File Transfer implementation. Both you and your partners are likely to have already invested in a variety of technologies related to encryption, file transfer, email, paging, and data management. A MFT solution needs to build on and interoperate with these existing technologies – not replace them.

Open technologies commonly involved in file transfers include FTP or secure FTP servers, HTTP or HTTPS servers, OpenPGP encryption or key servers, SMTP-compliant mail servers, or SQL databases. Clearly, both you and your partners would like to avoid replacing technologies that you have already implemented. For example, you would not want to add a second set of proprietary servers just for file transfer with one service provider or trading partner, when you already have secure FTP servers in place.

A best-in-class Managed File Transfer environment must comply with common standards and, most importantly, not force your partners to purchase proprietary, single-use technologies. In general, a Managed File Transfer solution should be transparent to your partners – requiring no changes in their business workflow or technology infrastructure. Aspects to consider when evaluating the open interoperability of Managed File Transfer solutions include whether it provides standards compliance and vendor neutrality.

Standards Compliance

Standards compliance for file transfer means you can exchange files with companies that support the same standards. Many Managed File Transfer products support open standards at this level of compliance. For example, if you own an FTP server and your trading partner owns an FTP client, they can send files to you or receive files from you via FTP.

Since you are likely to add new file transfers with additional service providers or trading partners to your Managed File Transfer solution over time, it needs to support a broad range of standards. Check to see if your proposed MFT solution supports transfer of a variety of file types (e.g., text, image, audio, and video), file sizes, and that it supports open standards, such as:

FTP, SFTP, FTPS, email, HTTP, and HTTPS for file transfer

SMTP for email notifications

OpenPGP for file encryption

SQL for audit or other databases

Vendor Neutrality

Your choice of a Managed File Transfer solution should not force your service providers or trading partners to invest in a solution from a particular vendor or “agree” on a solution. Your MFT solution should either interoperate with your partners’ current infrastructure or allow them to select any off-the-shelf product that supports the standards in your Managed File Transfer solution.

Managed File Transfer products that require your service provider or trading partner to implement a proprietary or single-vendor solution do not meet the requirements for a best-in-class solution. Commitment to vendor neutrality may mean that you must forgo certain features and functions that are technically feasible only with proprietary solutions. As an example, many secure file transfer vendors have added features to their products in response to market demand for more workflow capabilities. Some of these features require both you and your partners to install and support the same proprietary software.

3.2 Workflow Management

Workflow management is the wrapper around secure file transfer. File transfers are part of a business process. For example, transferring a payroll file to your payroll processing vendor is not just about the technology required to move the file from point A to point B. It's also about ensuring that the files are delivered accurately, completely, and on a specified schedule.

When you design a file transfer management process, take workflow management into consideration. Designing the workflow that surrounds secure file transfer includes consideration of requirements for real-time job monitoring, comprehensive audit capabilities, event notification, plus rapid containment and recovery.

Job Monitoring

File transfer is an inherently error-prone process with many moving parts. Eventually, even a best-in-class Managed File Transfer solution will have a problem with a file transfer. The hallmark of a good Managed File Transfer solution is the ability to monitor, diagnose and address file transfer problems before they become business problems.

Managed File Transfer solutions need the ability to monitor and manage file transfer jobs while they are running. If a problem occurs with an active file transfer job, the job may need to be cancelled. For example, you may need to cancel a job that is hung due to a technical problem. Or, a trading partner may contact you during a large file transfer and ask for it to be cancelled due to problems on their end of the transfer.

Once a job has completed, the first step in diagnosing a file transfer problem is being aware that the failure has occurred. As discussed above under Notifications, a good Managed File Transfer notification system delivers information that can be used to diagnose the problem to the person who can address it.

A good Managed File Transfer solution also supports tools to assist with troubleshooting file transfer jobs:

- Log files with extensive, informative entries. Since entries to log files are written sequentially in the order they occur, log entries from different jobs are typically intermixed in the file. When multiple jobs were executed at the same time, it is difficult to sort out the status of any individual file transfer by looking at the log in its standard format.
- Log analyzer to view and analyze a log file to assist the user in understanding and troubleshooting the results of a specific file transfer's events. For example, if you want to check the exact steps that occurred in a particular job, a log analyzer would allow you to search for and display only the log entries related to that particular job. Or, if a specific error occurred, such as an audit trail failure, a log analyzer would help you locate the log messages related only to that failure.
- Reporting tools to diagnose “system-level” problems, in addition to diagnosing individual file transfer problems. For example, say you exchange files with two trading partners. Audit data can be used to identify whether any particular failures, such as FTP login errors, occur mainly with one trading partner. If so, you or the affected trading partner may need to adjust file transfer settings – e.g., changing FTP server settings to allow more concurrent logins.

Audit Capabilities

Because of the growing emphasis on regulatory compliance, most companies need to capture a flexible, extensive set of audit data as part of their business process. When considering a Managed File Transfer solution, identify all of the data you need for internal reporting and external compliance; and, make sure the solution can capture it.

Audit data from a Managed File Transfer solution frequently needs to be integrated into a corporate compliance data infrastructure. Managed File Transfer solutions make it easier to integrate file transfer information into the corporation's compliance and reporting processes by using standard approaches such as SQL databases.

Audit data is critical to some companies and less essential to others. If you have a hard-and-fast requirement

Event Notifications

When a file is transferred between you and a trading partner or, perhaps, a remote office, the individual sending the data and the individual receiving the data need to know that the process is working as expected. Event notification enables your IT personnel, your business users, and your partners' business users to stay informed of the status of a file transfer.

The notification capabilities of a Managed File Transfer solution should be assessed on three dimensions:

- Flexibility. Event notifications need to be flexible enough to serve the needs of different types of users, both in your company and at your remote office, service provider, or trading partner. For example, a business user might need notification if a file transfer has succeeded; whereas, an IT support person might need notification if a file transfer fails, so that he or she can correct the problem. Quick problem resolution is particularly important in cases where the arrival of a file is required at a specific time, such as month-end financial data from hundreds of remote branches that is due to the corporate accounting department by 5 p.m. Eastern Time on the 6th of each month.

- Targeted content. Different types of users require different information in their notifications. Business users, for example, are typically concerned with top-level information on the success or failure of a file transfer, whereas IT support personnel need detailed technical information on the attempted file transfer, in order to diagnose and correct problems.

- Delivery options. Determine whether the Managed File Transfer solutions you are evaluating offer some options in notification methods – email and paging are two examples. If a time-critical file transfer fails, you may want the IT person responsible for file transfers to receive an email and the "on call" IT person to be notified by pager.

Containment and Recovery

IT emergencies are as unavoidable as they are undesirable. File transfers are business-critical for most companies. When an IT emergency occurs, file transfer jobs need to be back online as soon as possible. Look for Managed File Transfer solutions with simple, integrated backup and recovery capabilities for a fast response in case of an emergency or the ability to automatically roll over to a hot stand-by system.

When a security breach occurs at either your company or a partner's site, you need to be able to respond to it immediately. You must be able to contain the breach by shutting down affected file transfers immediately and restarting them when the breach has been addressed. A Managed File Transfer solution should allow you to suspend transfers in a variety of ways, such as all file transfers, file transfers with an affected trading partner or FTP server, or file transfers using a particular encryption key.

At times, you may need to recover or recreate an individual file transfer. Perhaps you need to resend a file to a service provider or trading partner that inadvertently lost or deleted a file. Or you may have legal or regulatory guidelines that require you to retain files for a specified length of time. You may choose to retain files in their plaintext format, their encrypted format, or both. A Managed File Transfer solution must be able to archive files that have been successfully transferred, so that these files are available for review or retransmission to meet your workflow requirements.

"While 'secure transfer' solutions are adequate for some data transmissions, Managed File Transfer suites address security protections but also tackle a company's internal and external auditability accountability and data control requirements..."
– Gartner Research

Secure File Transfer

Secure file transfer is at the heart of a Managed File Transfer solution. Aspects to consider when evaluating the secure file transfer component of Managed File Transfer solutions include whether it provides **end-to-end data security, 24x7 automation and in-process error correction.**

End-to-End Data Security

Your corporation's data security policies are the foundation of a secure file transfer process. Data security policies should require that all data files are protected before leaving the corporate data center. In particular, files that are outside the corporate firewall in a DMZ must always be encrypted. File transfer solutions that wait to encrypt data until it is on an FTP server in a DMZ outside the corporate firewall create a gaping security hole.

For end-to-end security, your Managed File Transfer solution needs to support:

- Level of encryption needed to protect data-at-rest and data-in-motion. Some situations may call for only a moderate level of protection, such that standard encryption algorithms with low bit-levels are adequate. Other situations may require up to 4096-bit keys with the most sophisticated algorithms supported by the current OpenPGP specification.

- Choice of which secure FTP to use to protect data during transit – SFTP (SSH) or FTPS (SSL). Each provides similar levels of protection for FTP login data, as well as for data files being transferred. FTPS is a narrowly defined protocol applicable only to file transfers. SFTP implements a secure shell that can be used in a variety of applications. SFTP can be more difficult to implement and maintain, as it needs to be tailored to ensure that each user account is restricted only to the file transfer features it requires.

- Use of data encryption. Neither SFTP (SSH) nor FTPS (SSL) protects data-at-rest. For data to be secure, files need to be encrypted before being transmitted, even if a secure FTP protocol is being used. If a file is not encrypted before transmission, it will be plainly visible as soon as it reaches its destination. Unencrypted files on an FTP server in your or your partner's DMZ can be a major security loophole.

- Security of the Managed File Transfer application itself. Data security policies cover data beyond the files being transferred. Data used during the file transfer process (e.g., pass-phrases or log-in data) needs to be protected, as well. To prevent theft of this critical data, it should never be written to disk in plaintext by a Managed File Transfer application. Look for solutions that require password-protected logins and automatically encrypt sensitive data (e.g., pass-phrases and login data) before writing it to disk.

- Authentication to guarantee the identity of the sender. The file might be from an unknown source and, therefore, have unreliable or dangerous content. For example, a bank might receive a data file from an insurance company containing data for claim checks that indicate payees and amounts to be distributed. Although the file might arrive at the expected time and decrypt with the correct private key, without authentication you might process the file and only later discover that it did not come from your partner.

- Authentication to prevent file corruption or tampering while in transit. A file may appear to arrive encrypted and unharmed, but the only way to be sure is to sign and verify the file. If the contents of a signed file are changed in any way, the signature will not be authenticated successfully. A business practice requiring partners to sign each file before sending, and authenticating their signatures when you receive the file, prevents these kinds of errors.

24x7 Automation

A good Managed File Transfer solution integrates smoothly into your production environment. Most IT organizations evaluating Managed File Transfer solutions are strongly motivated by the desire to improve their ability to automate file transfers, primarily because they have experienced the overhead and errors created by manual processes. They also know that as transfers grow, the potential for errors also increases.

Your Managed File Transfer solution must have the flexibility to meet not just your, but also your service providers' or trading partners', automation requirements. When you exchange files with partners or remote sites using an automated process, these requirements must be handled by your Managed File Transfer solution.

For example, your partner may configure its FTP servers such that it cannot receive binary files. Since all encrypted files are binary, your partner may insist that you ASCII-armor all encrypted files before sending them to the FTP server. Or, your partner may plan to use a file that you created on a Microsoft® Windows® platform on a Unix system. If so, you must convert files to a canonical format before encrypting them. Otherwise, your partner's systems may not be able to process the file correctly after decryption.

You or your partners may have business rules that need to be followed. You may choose to leave older files on your FTP server and want to overwrite them as new files are sent. Or, if you are downloading files from a partner's FTP server, they may want you to delete files that have been processed to prevent the possibility of downloading the same file twice. Your partner may also want files that you send to conform to their internal naming convention – rather than your naming convention. In this case, your MFT solution needs to be able to rename files during the file transfer process.

The final aspect of automation is job scheduling. A good Managed File Transfer solution should offer flexible, integrated job scheduling that eliminates the need to use third-party scheduling tools (e.g., Microsoft® Windows® Task Scheduler). File transfers may need to be scheduled at specific times of the day, week, or month to match your workflow requirements. Or, files may need to be processed on an irregular schedule as they become available. Good automated scheduling in a Managed File Transfer solution allows you to execute each job at the right time without relying on other job scheduling tools.

A Managed File Transfer solution should have:

Flexible, integrated job scheduling that allows the Managed File Transfer solution to operate independently of other applications or job schedulers.

Job execution via scripts or a command line interface that allows simple batch jobs to initiate file transfers, when you have job streams that need to execute a secure file

In-process Error Correction

Automation can be a great time-saver, as long as other errors do not creep into your file transfer process. For example, when processing files with payroll or insurance claims data, your Managed File Transfer solution should ensure that a file is not processed more than once. Or, you might want to validate that the file you receive is the file you requested, by checking that the file passed to you by an FTP server is the same size as the file that you were expecting to receive. A good Managed File Transfer solution automatically prevents these common errors, so they are addressed without manual intervention during the file transfer process.

Although many file transfer errors cannot be corrected “in process," some errors can be. A good Managed File Transfer solution automatically handles common, transient errors during a file transfer. For example, if the Managed File Transfer application is unable to log in to an FTP server, it should automatically reattempt several times before giving up. Another file transfer error is when the file received from an FTP server is not the same size as the file that you requested. Your MFT solution should attempt to check the size of a file before downloading and ensure that the file after downloading matches the original file size.

Multi-file jobs can create additional “in process” problems. When a file transfer job attempts to download multiple files, some files may download and decrypt correctly, while others may fail. A good Managed File Transfer solution continues to process all files in a job, even if one or more files fail to complete without errors.

3.4 Scalability

Scalability is the final essential element of a Managed File Transfer solution. Managed File Transfer is no different from other applications in its requirement for scalability. The number of file transfer jobs your organization handles will increase as your customers, remote sites, and partners increase their security requirements and expand their automation of business processes – including secure file transfers. You'll want to evaluate a Managed File Transfer solution's scalability on performance, maintenance, and reuse.

Performance

Because the performance of your Managed File Transfer solution can be adversely affected as you add more file transfer jobs, your solution must be architected to deliver sustained high performance as file transfer volumes increase. Look for easy, transparent migration to new hardware platforms.

For example, solutions with client/server designs allow the backend server software to migrate to higher-performance systems without impacting clients already in place. Also, the scheduler in your Managed File Transfer solution should be multi-threaded, so that each file transfer job spawns a new thread – allowing as many jobs as desired to run concurrently.

Other performance-enhancing features include compression of files for improved file transfer times and automatic retries of file transfer tasks without restarting the entire file transfer job. For example, if an FTP connection fails during a file transfer, a Managed File Transfer solution should attempt to reconnect without restarting the entire job. This action saves time as file encryption and other file transfer job steps do not need to be repeated.

Maintenance

Maintenance tasks can increase dramatically as the volume of file transfers increases. For example, workflow process rules may require that you retain archive files for a period of time. In this case, your Managed File Transfer solution needs to include a simple, automatic way to set retention periods and automatically delete files at the end of the period to prevent the buildup of unnecessary files.

Other MFT-generated files, such as log files, can also get out of hand with large volumes of file transfers. Some Managed File Transfer products create log files but do nothing to maintain them. As these log files become extremely large, they can slow down or even cause the application to fail. Even if your Managed File Transfer solution generates new log files on a regular schedule, the sheer number of log files can become unmanageable.

Ensure that your Managed File Transfer solution has built-in tools to prevent log files from becoming too large and that it automatically cleans up out-of-date archive and log files.

Re-Use

Scalability is also enhanced when you can reuse file transfer information as you set up new file transfer jobs. Your Managed File Transfer solution should allow you to specify partner profiles with FTP parameters and encryption/decryption keys to be used across all file transfers with that partner. Also, you should be able to modify file transfer jobs that you have already set up to create new file transfers – re-entering only changes to the file transfer data.

4 | Managed File Transfer Comparison Chart

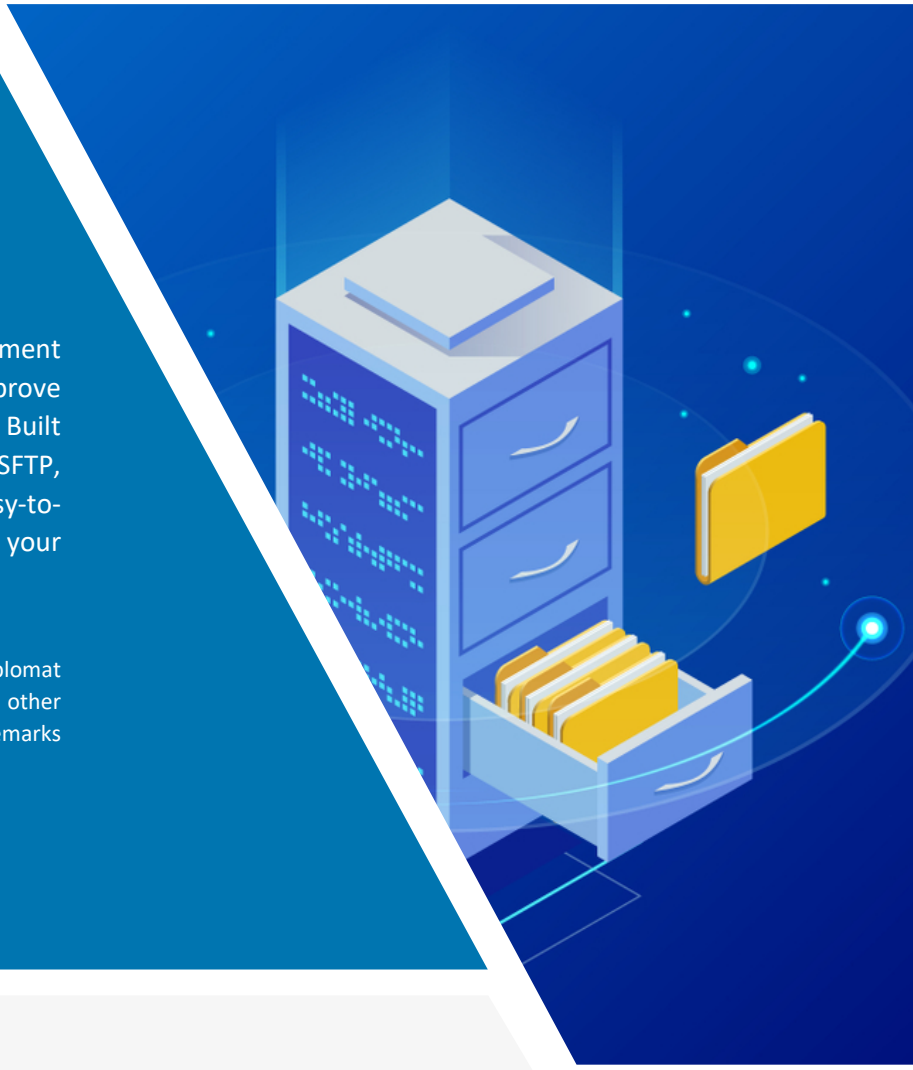
Coviant Software delivers scalable, file transfer management solutions that integrate secure file transfer with critical workflow processes. Diplomat® Transaction Manager, Coviant Software's file transfer management suite, provides extensive features and exceptional performance at an affordable price. The following checklist lets you compare other file transfer management solutions with Diplomat Transaction Manager from Coviant Software.

Managed File Transfer Comparison Chart		Diplomat	Other MFT Solution
Open Interoperability			
Standards Compliance	Complies with standards-based solutions you and your partners have in place (FTP, SFTP, FTPS, HTTP, HTTPS, OpenPGP, SMTP, SQL)?	✓	
	Supports a wide range of file sizes and types?	✓	
Vendor Neutrality	Works with partners' file transfer solution of choice?	✓	
Workflow Management			
Event Notifications	Notifies you and/or trading partner when a file has been successfully transferred?	✓	
	Notifies you and/or your trading partner if a file is not transferred by a particular time?	✓	
	Includes "right" information for each recipient – top-level information for business users and detailed technical information for IT personnel?	✓	
	Notifies "on call" IT personnel of urgent file transfer problems by email and/or paging?	✓	
Audit Capability	Creates audit trail database?	✓	
	Captures all required audit data, including user activity?	✓	
	Enables easy integration of MFT audit data with other applications?	✓	
	Allows suspension of all file transfers if audit data not being captured?	✓	
Recovery and Containment	Recreates MFT environment quickly and accurately in case of an emergency?	✓	
	Enables automatic rollover to a hot stand-by system?	✓	
	Allows easy suspension of all transfers in the event of a major security breach?	✓	
	Allows easy suspension of all transfers with an affected partner?	✓	
	Allows easy suspension of all transfers using a compromised key?	✓	
	Archives files for easy resend to partners?	✓	
Job Monitoring	Monitors active file transfer jobs with ability to cancel jobs and view detailed activity?	✓	
	Enables cancellation of active file transfer jobs?	✓	
	Captures system messages in log files?	✓	
	Provides log analyzer with search capabilities to read/analyze log files?	✓	
	Provides reports to help identify recurring file transfer problems?	✓	
	Includes troubleshooting information in notifications to IT personnel?	✓	

File Transfer Management Feature Checklist		Diplomat	Other MFT Solution
Secure File Transfer			
Data Security	Supports SFTP(SSH), FTPS(SSL), and HTTPS to ensure protection of login data and data-in-motion?	✓	
	Protects MFT application data with password login or network authentication?	✓	
	Encrypts sensitive data (e.g., pass-phrases or login data) automatically before writing to disk?	✓	
	Protects data-at-rest and data-in-motion with required bit-level of encryption?	✓	
	Protects data outside the corporate firewall (e.g., in your or your partner's DMZ)?	✓	
	Authenticates identity of sender?	✓	
	Validates file integrity to ensure contents are complete and unaltered?	✓	
Automation	Enables transfer of files on regular schedule – hourly, daily, monthly?	✓	
	Enables processing of files automatically as they become available?	✓	
	Offers integrated scheduling capability, such that third-party scheduler not required?	✓	
	Integrates MFT file transfers easily into existing job streams?	✓	
	Supports ASCII-armoring of files after encryption?	✓	
	Enables creation of canonical files before encryption?	✓	
	Allows or prevents overwrite of existing files when sending or receiving files?	✓	
	Enables selective deletion of specified source files after delivery to partner?	✓	
	Allows file renaming during transfer, such that partner can recognize files?	✓	
Error Correction	Reattempts file transfer tasks if FTP login error or a dropped FTP session occurs?	✓	
	Accepts files only after confirming size of file received is same as size before transfer?	✓	
	Documents problem and rolls back to original state, if problem occurs during file transfer?	✓	
	Continues processing remaining files in job even if a problem occurs with one or more files?	✓	
Scalability			
Performance	Supports increases in file transfer volume without creating performance bottlenecks?	✓	
	Enables transparent migration to higher performance platforms?	✓	
	Compresses files for improved file transfer times?	✓	
	Enables independence of management console and run-time job processing engine?	✓	
Maintenance	Deletes archived files automatically based on schedule you set?	✓	
	Deletes old log files automatically based on schedule you set?	✓	
	Creates new log file automatically when active log file reaches a certain size or age?	✓	
Re-use	Allows creation of partner profiles with file transfer login information and encryption/decryption keys to be used across multiple file transfer job specifications?	✓	
	Creates new file transfer jobs by modifying existing jobs?	✓	

ABOUT COVIANT SOFTWARE

Coviant Software delivers secure file transfer management products that secure data in transit and improve compliance with industry and government mandates. Built on open technologies, such as OpenPGP encryption, SFTP, and SQL, Coviant's Diplomat MFT platform is an easy-to-implement, cost-effective solution for automating your secure file transfer process.



5804 Babcock Rd / Suite 151 / San Antonio, TX 78240 /
210.985.0985 / info@coviantsoftware.com/
www.coviantsoftware.com