COVIANT Software

WHITE PAPER

Managed File Transfer:

When Data Loss Prevention Is Not Enough
Moving Beyond Stopping Leaks and Protecting Email

EXECUTIVE SUMMARY

Data Loss Prevention (DLP) monitoring products have greatly reduced the tidal wave of sensitive information flowing out of organizations. They inspect data-in-motion and identify network traffic that needs protection. With a little incremental effort, they can integrate with secure email tools to protect email messages and attachments containing sensitive information.

If you have a DLP implementation in place or are considering one shortly, your data-in-motion should be safe, right? Not exactly.

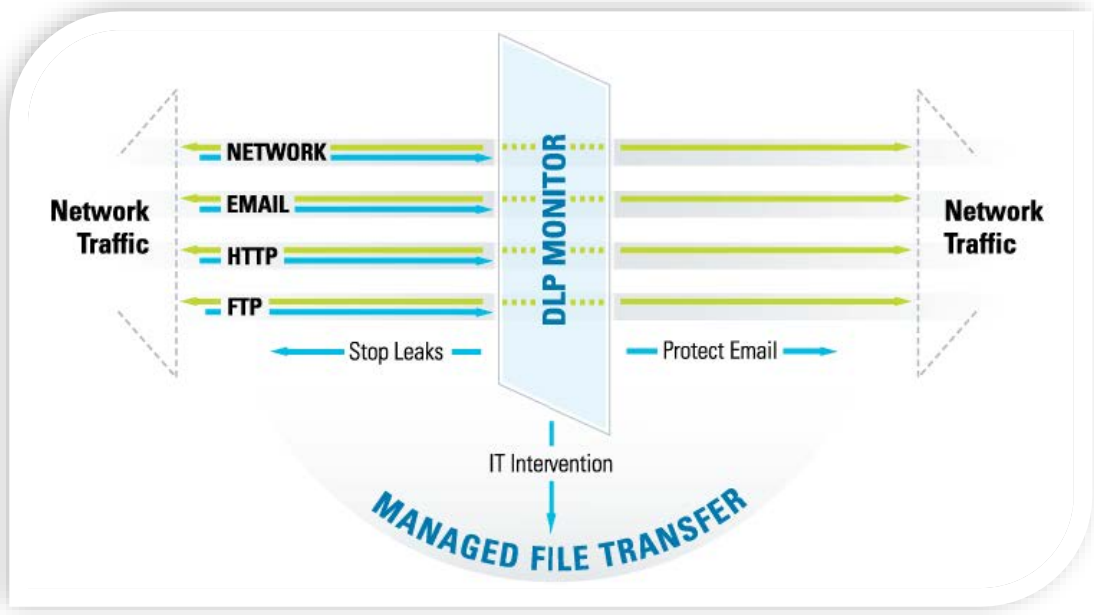
Protection of data-in-motion goes beyond stopping leaks and protecting email. You need to safeguard all types of network traffic containing sensitive information. Your content-aware DLP product can inspect and filter the flood of outbound traffic that your employees generate every day. It can identify sensitive information to stop leaks and can usually redirect email for more secure delivery. It can also identify high-risk network traffic that needs to be sent with a more secure process, but it cannot deliver it safely.

Managed File Transfer solutions specifically address the high risk data-in-motion that your DLP product can only identify, but cannot adequately protect. You can meet your business requirements for monitoring, enforcement, and auditing of high risk data-in-motion by using a Managed File Transfer (MFT) solution to provide a secure, authenticated delivery process for your most critical information.

The drawback? Ensuring locked-down delivery of critical information requires intervention. When your DLP product identifies high risk traffic, your IT staff needs to first confirm that these transfers are required to support your business operations and then determine exactly what information should be sent? When should it be sent Who is a valid sender? Who is a valid recipient? How can you reliably authenticate the recipient?

Once your IT staff confirms the validity of sensitive network traffic, they can use a Managed File Transfer solution to specify, protect, and control future transmissions. A one-time intervention lets you automate your most critical transfers and monitor them to address problems when they do occur. Over time, the number of interventions will decrease as your MFT solution handles more and more of your sensitive information.

This white paper reviews how Data Loss Prevention products can identify high-risk network traffic that requires intervention and how your IT staff can use a MFT solution to reduce your business risk from these transfers. Managed File Transfer products enforce your security policies, provide visibility and monitoring of ongoing transmissions, collect data for internal and external audits, and integrate with your current DLP solutions and other infrastructure applications.



1 | Managed File Transfer: A Critical DLP Component

In today's interconnected economy, businesses exchange information electronically with their partners, customers, and providers with increased frequency. It has become a daily, hourly, even minute-to minute activity for most organizations. Everything from your customer list to payroll data is now transferred online.

This relentless ebb and flow of data-in-motion constantly expands your business risk. Non-compliance with government and industry mandates can trigger high notification costs and regulatory fines – not to mention criminal penalties. And, the publicity from a data leak can be disastrous for your company's reputation.

You must put safeguards in place to reduce your business risk in the face of this explosion in data-in-motion. A content-aware DLP product is your first line of defense. It monitors and categorizes your network traffic. Most traffic is delivered unimpeded. Some traffic is flagged and transmission is prevented. Sensitive email is frequently handled by a secure email tool that encrypts email content, redirects the encrypted content to a secure location, and sends notification email informing the recipient that the content is ready for pick-up.

IT intervention is required when sensitive content is transferred on a regular schedule, especially to the same recipient. Your IT staff must intervene to validate the sender, validate the receiver, and design and implement an automated, authenticated managed file transfer process to meet your business needs.

Although secure email capability for data-in-motion is offered by most DLP products or through their partner offerings, Data Loss Prevention products do not offer Managed File Transfer capabilities. DLP products can identify high risk network traffic, but do not offer an out of-the-box solution to design and manage a secure, authenticated file transfer process. When more protection is needed, you need to implement a Managed File Transfer solution – to go beyond what your DLP implementation can provide.

DLP products, secure email tools, and MFT solutions must work together to protect the sensitive information in your data-in-motion while effectively managing your business risk.

> "Many DLP implementations fail because blocking transmission is counterproductive to the legitimate business needs of sharing data with partners, customers, and investors."
>
> Ogren Group

2 | When is IT Intervention Justified?

When a Data Loss Prevention product identifies sensitive data-in motion, you would prefer a way to transparently protect and deliver it. You want to limit manual intervention that could result in business interruption. After all, data-in-motion is essential to your business. Payroll files must be sent to your bank. Design documents need to be transmitted to your manufacturing plant. And, this information must be delivered in a timely, but secure, fashion.

Secure email tools can partially address this desire for transparency. But encryption and redirection of email is only safe if the volume, frequency, and predictability of sensitive content are all low and authentication is not critical. In addition, secure email cannot protect sensitive information in HTTP, FTP and other network traffic.

All types of sensitive data-in-motion that occur with high volume, frequency or predictability or that require authentication need to be tightly controlled. These high risk transfers must be suspended so your IT staff can intervene to set up a process to protect your high risk data-in-motion using a Managed File Transfer solution for current and future transmissions.

2.1 Content Risk

When your DLP product identifies sensitive content, it can categorize the data-in-motion as either high or low risk.

High risk data-in-motion (e.g., trade secrets) has a critical core business value or such stringent regulatory penalties that it is better to intervene in such transfers than allow them to complete. The risk of even a one-time transfer of your trade secrets or upcoming product plans to unauthorized persons greatly outweighs the risk of a temporary business interruption.

Most sensitive information is less risky. Typically, it is needed to support valid business processes (e.g., payroll, order processing, and customer lists). Although the content must be protected, it also must be shared in order to run your business. You do not want to hamper normal business operations, but you do need to minimize business risk.

With less risky content, it is not always obvious whether intervention is warranted. Can you encrypt and redirect email or do you need to intervene and set up a highly controlled process? Further understanding of the context – volume, frequency and predictability – of the transfers are part of this equation. They need to be balanced against the potential business interruption before you can decide.

2.2 Context Risk

When information is moving within your network or to outside locations, you need to look not just at the content of the individual transfers but at the context, such as the volume, frequency and predictability of these transfers over time

The first time your DLP product finds an email message containing a few Social Security numbers, it might be reasonable to consider this a low risk transfer and use a secure email tool to encrypt and redirect to the recipient. This limited risk does not warrant the cost to research whether or not it is a valid transmission and to set up a Managed File Transfer process. But consistent monitoring of the email messages between the same sender and recipient over time might detect that the total number of Social Security numbers has reached an unacceptable limit and a Managed File Transfer process needs to be established.

Your DLP product also needs to monitor the frequency of transfers to the same recipient – whether or not it's from the same sender. The risk of one such transfer may be low. But if ongoing monitoring detects many transfers containing credit card numbers, it is possible that someone is intentionally stealing credit card numbers or that you need to intervene and set up a formal file Managed File Transfer process between your organization and the recipient.

Transfers with similar sensitive content going out on a regular schedule, especially if they originate from the same sender, need to be monitored. Predictable transfers can be anticipated and intercepted by unknown recipients. If you continue to encrypt and redirect with a secure email tool, a notification email to the recipient with both the location of the encrypted file and the key to access it become more and more likely to be intercepted.

2.5 Identity Risk

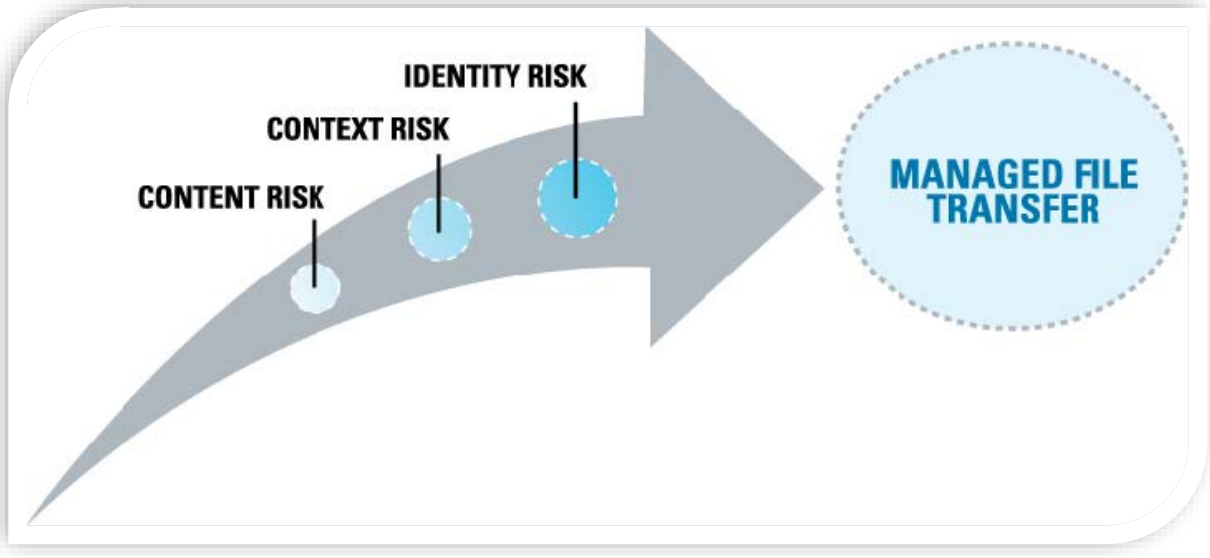
When you use a secure email tool, it typically uses a single key or password for encryption. This key or password is then forwarded to the recipient along with information on the location of the encrypted file. In this scenario, there is no way to ensure that the person receiving the content is the intended recipient. Anyone who intercepts the email with the key or password and instructions on how to access the encrypted file can access the sensitive content you are trying to protect.

More secure processes require validation and authentication of the identities of the sender and recipient – which is critical to protect data-in-motion from falling into the wrong hands and being used for purposes such as identity theft or unauthorized credit card purchases. Validation ensures that sensitive content is appropriate for the intended recipient. Authentication ensures that the actual recipient is the same as the intended recipient and that no other recipients are able to access the content.

Validation determines if the sender and receiver are appropriate for the information being transmitted based on defined, enterprise specific policies. Your DLP implementation can have rules that determine whether the sender and recipient are known to be "valid" for the type of information being transmitted. For example, an email containing payroll information coming from someone in your payroll department and going to an email address at your bank might be considered to have a valid sender and receiver. Conversely, you might have a rule that suspends all transfers of payroll data from email addresses outside the payroll department.

If your DLP product confirms that an email has a valid sender and receiver, it might be appropriate to use a secure email tool to transparently encrypt and send the information. But intervention would be required to be certain that the person or process receiving the transmission is the intended recipient.

Authentication requires the identities of both the sender and recipient be confirmed. Each party needs to provide the other party with information verifying their identity. Typically, this is accomplished by exchanging public keys before sending sensitive content. After receiving the recipient's public key, the sender encrypts the content using the recipient's key and signs the encrypted content with his or her own private key. The resulting signed and encrypted file can be safely transmitted to the recipient. The recipient confirms the content really did come from the sender by verifying the signature on the encrypted file using the public key of the sender. Then, the recipient decrypts the content with his or her own private key. Since only the recipient has the private key matching the public key sent to the sender, the sender is assured that only the intended recipient will be able to access the sensitive content.



3 | Why Managed File Transfer?

Transfers with high content, context and identity risk need to be tightly controlled to meet both business and security requirements. Managed File Transfer solutions not only protect sensitive content, but provide ongoing visibility, monitoring, enforcement, and auditing of the file transfer process while integrating with your IT infrastructure.

When your IT staff does have to intervene in the transfer of data-in motion, Managed File Transfer solutions let them set up a safe automated process for handling future transfers. And, your DLP product can be configured to recognize MFT solutions as trusted senders of encrypted content. A one-time investment means your business processes will not be interrupted in the future.

3.1 Policy Enforcement

Precise policies on how to handle secure file transfers vary, but full protection requires a combination of file encryption, secure transfer protocols, and authentication.

Sensitive content needs to be encrypted before it leaves the corporate firewall since secure transfer protocols only protect data-in-motion. Adhering to a strong encryption standard, like OpenPGP, offers security when data reaches its destination. OpenPGP ensures that only the intended recipient can access the file content and it uses advanced encryption algorithms (e.g., AES-256 and SHA-512) for enhanced data protection.

Files with sensitive content can be signed to confirm the identity of the sender. Without a signature, the source of a file is unknown. It could have been tampered with in transit or intentionally contain malicious content. When recipients successfully verify the signature on a file, they can be sure of the identity of the sender.

File encryption protects your content, but does not protect the logon information used to access an FTP or HTTP server. Security can be enhanced by using secure protocols, such as SFTP (SSH), FTPS (TSL/SSL), or HTTPS (SSL) to protect both login information and file content. These secure protocols establish a secure connection before sending the logon information used to authenticate the user, such as username and password. Thwarting access is a critical security concern. If attackers capture logon information, they can initiate other file transfer jobs and potentially transmit files with malicious content.

3.2 Visibility and Monitoring

Transfers of sensitive content occur on a regular basis. Files may be transferred on a schedule or on an ad-hoc basis throughout the day as they are ready to be processed. A Managed File Transfer solution automates file transfer jobs, integrates with other business processes, provides real-time monitoring of file transfers, and sends notifications about file transfer results.

Automation of secure file transfers reduces errors and limits access to sensitive content. MFT solutions allow login and encryption information to be entered once and accessed as needed at run-time. MFT applications always have the correct encryption key and logon information which eliminates the possible introduction of security errors into the file transfer process.

Visibility of secure file transfers is critical. Monitoring file transfer jobs with a MFT solution rapidly identifies potential security problems. Automating file transfer jobs does not guarantee that no issues will arise at run-time. A job not running on schedule or taking too long to complete may signal a problem. When a file transfer job fails, the responsible support person needs to be alerted as soon as possible. Email or paging notifications need to be sent. If a security breach occurs unrelated to a file transfer (e.g., an FTP server or encryption key has been compromised), the specific file transfer jobs affected may need to be suspended until the security breach has been corrected.

3.3 Auditing

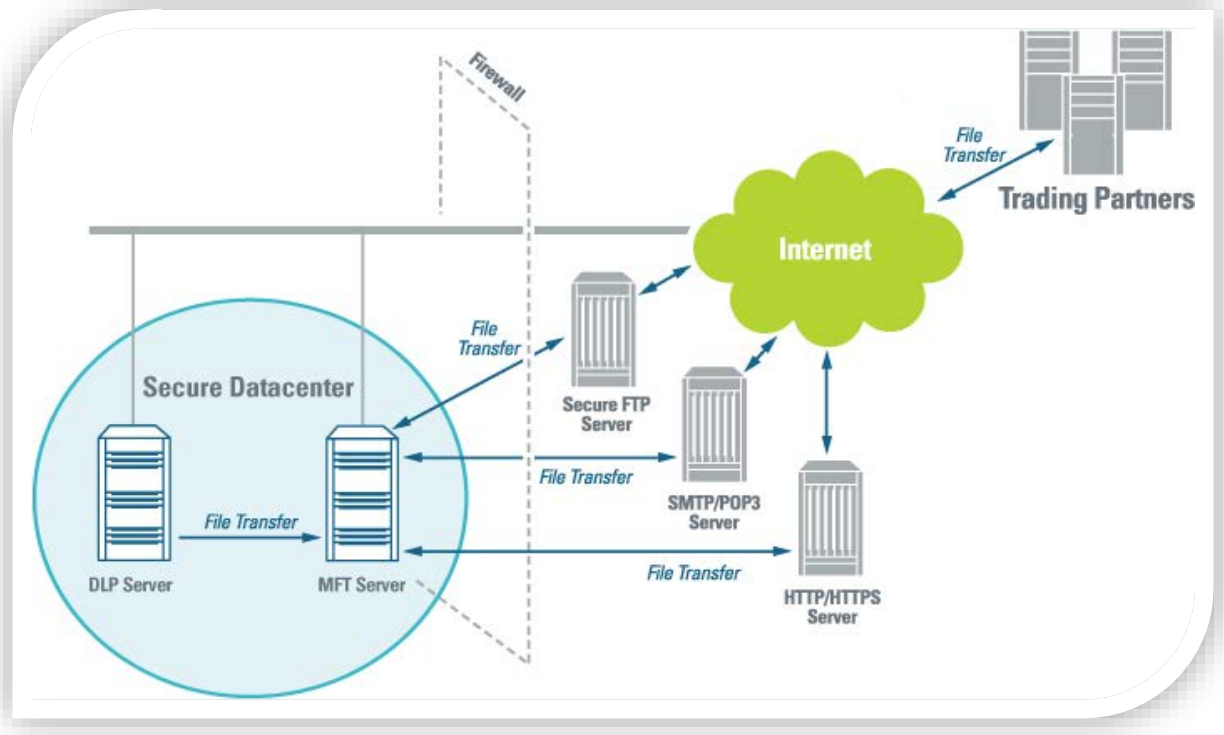
Detailed audit data is required to demonstrate regulatory and internal audit compliance, but proving you have a secure file transfer process can be an arduous task. Audit data needs to be both comprehensive and easy to analyze.

Your Managed File Transfer solution needs to capture both job and user activity information. Detailed data on each file transfer job can demonstrate that secure procedures, such as encrypting files before transfer and use of secure transmission protocols, were used for each file transferred. User activity data, data on who accessed your file transfer solution, is equally important. If files were transferred incorrectly, questions of who may have set up or updated the file transfers may become critical.

3.4 Workflow Integration

Transfer of sensitive content needs to be integrated with your overall business workflow. A MFT solution should be flexible enough to manage workflow by itself or in combination with other applications. For example, you might need to kick off a post-processing job once files are received or run a job just before files are transferred. Or, you may have a process where another application needs to initiate a file transfer job as part of a larger business process.

Your Managed File Transfer solution should enhance your existing technologies, not replace them. A MFT solution should leverage your current IT infrastructure by being vendor neutral and supporting common industry standards. Typically, MFT solutions work with technologies that you already have in place, such as FTP or secure FTP servers, OpenPGP encryption, SMTP or POP3 email servers, HTTP or HTTPS servers, and SQL databases. Plus, choosing a Managed File Transfer solution that adheres to industry standards will limit the impact on your trading partners' IT processes.



4 | Conclusion

Managed File Transfer solutions work with Data Loss Prevention products and secure email tools to provide a complete solution for identifying and securing your data-in-motion. DLP products can use intelligent security policies to identify data-in-motion that needs to be secured by a MFT solution. Deployed together, DLP and MFT solutions can minimize your business risk by limiting your liability from regulatory penalties, preventing exposure of your company's highly valuable assets, and protecting your company's reputation.

By reviewing the content, volume, frequency, predictability, and identity attributes of data-in-motion, DLP solutions can identify which transfers require a one-time IT intervention to set up a MFT solution. Content that is transmitted frequently and predictably in significant volume over time or when senders and recipients must be validated and authenticated present the most business risk. A visible, controlled process that enforces security policies and integrates with your business workflow is required to protect this content. Managed File Transfer applications work together with Data Loss Prevention products to protect your most sensitive data-in-motion.

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