WHITE PAPER

Best Practices in Data Loss Prevention Deployment for MFT

Protecting Your Organization's Mission-Critical Information

Cleo™

Move View Act®

Table of Contents

Introduction: Data Loss Prevention Best Practices for MFT

The possibility of sensitive data inadvertently leaving an organization is an ever increasing danger to enterprises of all sizes. Confidential information, whether Research & Development (R&D), financial, Personally Identifiable Information (PII), Protected Health Information (PHI), Intellectual Property (IP), Payment Card Industry-Data Security Standard (PCI-DSS), usernames/passwords, personal contact information is ubiquitous within every business. Protecting this information from exposure is core to ensuring your reputation and brand, and further, can prevent significant financial loss from fines, audits and prosecution.

To address these concerns, many organizations have begun to implement "Data Loss Prevention" (DLP). This technology is designed to prevent sensitive information from inadvertently leaving the organization. DLP is a key component of an organization's GRC (Governance, Risk and Compliance) process. There are many DLP products on the market, though we will focus on content-aware DLP. Gartner, Inc. provides the following:

"Content-aware data loss prevention (DLP) tools enable the dynamic application of policy based on the content and context at the time of an operation. These tools are used to address the risk of inadvertent or accidental leaks, or exposure of sensitive enterprise information outside authorized channels, using monitoring, filtering, blocking and remediation features."

Synopsis

Organizations have considerable amounts of sensitive information flowing in and out of their business, and many have implemented Data Loss Prevention processes to prevent this information from inadvertently leaving the organization.

This white paper offers an in-depth view of the relevant best practices for preventing data loss as part of a managed file transfer solution in your operation.

Basic Tenets of Data Loss Prevention

There are two basic precepts when implementing DLP. First, utilizing DLP, do not allow sensitive data out of the organization unless it needs to leave. Second, for the sensitive data that is required to be transmitted, ensure comprehensive encryption of that data.

Many organizations overlook the massive amount of data that is sent automatically on an ongoing basis, day-in and day-out. At first glance, this data may seem to be completely free from DLP risk. However, organizations send considerable quantities of sensitive information to their business partners. Ensuring that the right information goes only to the appropriate partner is critical.

In general terms, data is produced by various personnel and/or systems within the organization which is then targeted to external partners. This data should first be scanned by a DLP solution, encrypted and transmitted to the external partner. However, in many organizations, the most sensitive information is encrypted as soon as it is created, making it impossible for a DLP solution to review the content and identify sensitive data. A comprehensive DLP deployment can address these and other issues.

Transmission Between Systems

Data can be leaked electronically via websites, email, systematic file transfers, social media and many other ways. Each method has its own exposure footprint. In this article we will focus on systematic file transfers. This is the automated transfer of data between two computers, or systems. For the purposes of this article, we will look at transmissions between systems in different organizations, where the potential risk of data "leaving" an organization is a given.

Thinking About Encryption

There are three different aspects of encryption to think about:

1. Encryption in transit: This is usually achieved by using a secure communications protocol to ensure that data cannot be intercepted by a third party when going to and from an organization.
2. Encryption at rest: Typically implemented to prevent unauthorized internal parties from accessing sensitive data on internal disk sub-systems. Such encryption is often implemented within a file transfer Gateway, encrypting files as they arrive in an organization and decrypting them before they leave.
3. Encryption of payload: Payload encryption implements encryption of the file content itself while in transit to or from an external party.

There are two varieties of payload encryption:

- Where encryption/decryption is handled by the file transfer Gateway.
- Where encryption/decryption is done outside the Gateway, and the Gateway simply transfers the encrypted files.

Each encryption technique can be implemented independently of each other, but sometimes a weakness in one area can be addressed by using another. So, for example, where unencrypted communications protocols need to be used for legacy purposes, organizations may use payload encryption to compensate.

Key considerations regarding encryption are:

- Always use secure communications protocols where possible. Where not, use payload encryption to ensure data is not exposed.
- For sensitive information, ensure it is encrypted at rest to make sure there is no accidental or deliberate access to data on disk by unauthorized personnel.
- Where payload encryption is mandated (either by partner or internal processes), perform encryption/decryption at the file transfer Gateway. In this way, processes that require access to file content (such as content-based routing, DLP, Antivirus, etc.) can gain access to the decrypted content.
- If end-to-end encryption (not performed at the Gateway) is implemented or mandated, consider including additional decryption keys in the encrypted message so that the Gateway can decrypt and analyze the file content as needed.

Designing Your Data Loss Prevention Deployment Strategy

It goes without saying that DLP processing can only be performed on un-encrypted data content. Therefore it is important to take this into account when designing your DLP and encryption strategy. In particular, if end-to-end encryption is used (encryption is not performed at the file transfer Gateway) it is not possible to perform DLP scanning without adding a decryption step, generally done by providing a secondary key, owned by the Gateway. In addition, if encryption at rest is used, the Gateway must have the capability to vector content to the DLP (using a standard protocol such as ICAP - Internet Content Adaptation Protocol) as it won't be possible to scan files directly from disk. So organizations with DLP requirements for outbound files must ensure these files are available at the right place in an unencrypted form or that the Gateway has the ability to decrypt them.

Many organizations have already implemented and are familiar with DLP deployments with email and/or web transfers. These types of data transfers are generally initiated by a person, making the data volumes much smaller than systematic file transfers. Thus, these manual transfers have much lower DLP overhead than systematic file transfers. Whether you utilize a single instance (cluster) of DLP or separate instances based upon data type and/or geography is a key consideration.

File size is also a factor to consider in designing a DLP deployment strategy. Vectoring content to a DLP server typically has a maximum practical file size – either in terms of what can be processed by the DLP solution, or what can be handled in terms of throughput by the ICAP protocol and/or server infrastructure running the DLP solution. You should work with your DLP vendor, file transfer vendor and security team to define these limits and how they can be aligned with overall security policies. In some cases, due to the number or size of files, you may choose to process only a subset of data through DLP.

While ICAP is a standard, and in general vectoring content to a DLP server using ICAP is also standardized, there is significant variation in how each DLP server responds to ICAP requests. You should ensure your solution is flexible enough to account for these variations.

Additional Considerations

Another consideration is whether or not you can clearly identify source systems that produce data requiring DLP and those that do not require DLP. The existing process for transmission can remain the same for the non-DLP required systems, reducing the overhead on your DLP servers. This will make for a more complex environment, but may pay for itself with lower licensing and infrastructure costs.

Key considerations regarding DLP for systematic file transfers include:

- Determine whether to send all source data or a subset of source data through DLP.
- When possible, utilize a standard process for all data going through DLP. - Ensure you have a strong case if you will be utilizing multiple process paths for various DLP and non-DLP data based upon data sensitivity.
- Implement separate DLP instances for each data type (email, websites, systematic, etc.).
- Implement separate DLP instances based upon geography
- If data is considered safe within the organization, simply encrypt at the Gateway following DLP.
- If encryption at the source is a requirement, provide a secondary decryption key for the Gateway. - Avoid having separate encryption and decryption for transfers within the organization, followed by DLP and a subsequent encryption for external transfers.
- If at all possible, integrate your file transfer Gateway directly with source systems to allow DLP/encryption/transmission in lock-step.

Summary

When looking to deploy a DLP solution for your systematic file transfers, you will have to do a deep analysis of your current environment, identifying all existing file transfers and systems. Once these have been cataloged, the more difficult task is to determine which of these require DLP.

Many companies conclude that the risk of not properly classifying data as to whether or not it requires DLP is too great of a risk. Additionally, a single process through a standard Gateway ensures simplicity, auditability and reliability in that process. These two decisions together will significantly reduce the risk profile of any organization.

Cleo can help you define the best DLP approach for systematic file transfers in and out of your organization, balancing the various architecture, risk and cost variables. Cleo can further integrate your DLP solution into an overall file transfer strategy, to meet your targeted GRC requirements.

Cleo™

Move View Act®