WhitePaper

Using FileOpen with Data Loss Prevention (DLP) to Control Documents

The increasing volume of a company's information assets that are distributed in digital form, combined with BYOD and use of tools like Dropbox, has created an ever-growing risk of information leakage. At the same time, organizations face pressure to accelerate business processes, which inevitably fosters the urge to distribute documents immediately and broadly in digital – sometimes in draft – form. Today's documents must be controlled both within and without the organization.

For over 15 years, FileOpen Systems has been developing tools to control document distribution. The FileOpen solution has by far the largest footprint in secure document distribution and clients, including a substantial number of the world's major financial institutions, publishers, governments and Fortune 500 corporations. A substantial number of these FileOpen licensees are now seeking to create comprehensive solutions encompassing Digital Loss Prevention (DLP) to monitor data flow in and out of the firewall, with FileOpen document-level security as an added layer of assurance.

Scenarios

DLP systems exist to prevent the inadvertent or accidental distribution of sensitive information, by controlling network exit points and monitoring data using content inspection. Outgoing emails are scanned for keywords associated with risk, and suspect emails are blocked from exiting the firewall.

This "dragnet" approach works in some instances, but fails to address more common scenarios in which employees have a legitimate need to share sensitive information with external parties (such as legal counsel, etc.) In those situations, DLP can do more harm than good by encouraging employees to find ways to circumvent the technology.

There are multiple scenarios in which a document containing confidential or proprietary information might need to be both controlled internally and distributed to an external party. In many such cases it is critical that any protection remain in force as the content circulates outside the original corporate environment. To take just a few examples:

- Documents pertaining to employee evaluations must be circulated but should be visible only to specific people in the Human Resources department, or sales figures must be analyzed but only by particular executives, etc.
- During a merger negotiation a spreadsheet must be sent to an external investment banker, but the confidential information must not be shared with any other employee of that investment bank.

- A laboratory notebook containing secret intellectual property must be delivered as part of a regulatory filing.
- Documents related to a legal proceeding must be made available to opposing counsel during the discovery process, but copying or modification of those documents must be prevented.
- System diagrams and engineering specifications must be shared with multiple bidders on a project, but only the winning bidder should be allowed to view the documents at the end of the bidding process.

These challenges have in the past been addressed mainly by legal frameworks – employment agreements, nondisclosure agreements, etc. However, legal agreements offer only the threat of a post-facto remedy, which may be inadequate. This is especially true in cases where an identical digital document was distributed to multiple people, making it very difficult to identify which of the recipients was responsible for the unauthorized re-distribution.

Likewise, these challenges cannot all be addressed by systems that control data only within the corporate perimeter, i.e. by the majority of DLP systems. In cases where documents must be shared with external parties, it is not a solution for the DLP system to prevent distribution, or to flag the fact that the document was distributed. But neither is it optimal, from the perspective of the enterprise, for the DLP system to allow the document to be distributed in unprotected form: the sensitive document is now outside the reach of the DLP system and can no longer be tracked or controlled. How should the DLP system manage the document once it has exited the original network and been delivered into the environment of a user whose network may have a different DLP system, or no DLP at all?

Applications

The functionality provided by FileOpen is commonly referred to as Digital Rights Management (DRM), though several other terms also apply, as discussed below. DRM systems, like DLP systems but even more so, are designed to manage an end-user's access to a document in a way that is essentially invisible to them. Unlike password security, DRM systems authenticate once and then manage access without any further direct interaction with the end-user. DRM prevents unauthorized access to documents by encrypting all instances of a file by default and granting permission only to those explicitly authorized by the document owner. The design goal of DRM software must therefore be a balance between effectiveness and invisibility. DRM software must operate in heterogeneous client-side computing environments, and yet provide content owners with a satisfactory level of security against loss.

The FileOpen software may be configured to provide the same basic functionality – controlling when and where and how and by whom documents are opened and accessed – in different modes, as appropriate to the environment to be supported. The FileOpen software provides the functionality of:

- *Internal Document Control, or Enterprise Rights Management (ERM),* in which users are employees who can be unique and positively identified, their identities having been issued by the administrator, e.g. via Active Directory or other directory scheme. In ERM environments the software footprint is effectively unbounded, as administrators have no restriction upon what software they may install on (their organization's) local machines – up to and including DLP software. Privacy issues, if any, are a matter of local (e.g. human resources) policy, and bandwidth for communication with the servers used to manage documents is always present, either in direct LAN access or via a VPN connection.

- *External Document Distribution to Affiliates, or Information Rights Management (IRM),* in which users have a relationship with but are not employees of the organization, e.g. professional services firms, contractors, auditors, etc. The identity of these users is established by means of access granted to a system resource (e.g. portal login, IP gateway, VPN) but the users' information technology environment may be managed by an external party, using applications and operating systems licensed independently of the organization. User privacy must be respected, i.e. not all content may be scanned or communications monitored. Bandwidth cannot be assumed and offline use may need to be supported.

- *Document Publishing, or Digital Rights Management (DRM),* in which users have a preliminary (evaluation, bidding) or temporary (contract, subscription) or commercial relationship (document purchase) with the content owner, therefore may not have been issued credentials or paired to a specific identity, so may need to be identified and managed anonymously, e.g. by machine context. Computing environments cannot be dictated, so a wide variety of platforms (Win, Mac, Linux) must be supported along with a lowest-common-denominator application mix. User privacy must be respected, and applications installed on the user machine, if any, cannot be perceived as intrusive ("spyware", "malware") or interfere with normal user operations. Offline permissions must be supported, indeed may the exclusive mode of operation.

In all of the above applications, FileOpen solutions go further than basic pass-along prevention by providing document owners a rich set of permission features, such as the ability to set expiration, limit or prevent printing, and apply user-identifying watermarks to the digital and/or printed version.

Integration

A fully functional DLP system should be able to not only identify content but also manage the use and distribution of that content, both within and beyond the boundaries of the enterprise. In cases where documents must be distributed externally – the IRM and DRM cases above – the DLP system should support functionality to encrypt the content prior to external distribution, then manage and log the use of that content in the external environment. Adding DRM extends DLP functionality from a boundary solution into a complete document control/management solution.

It is possible to create a system that provides inward-facing DLP functionality and outward-facing IRM/DRM functionality, with varying levels of integration and automation. For example:

- The IRM/DRM component can be added as an independent capability with user interaction (e.g. sensitive documents found at the gateway in unencrypted form are returned to sender with instruction to re-send after encryption using the DRM system from within the document creation application).

- The IRM/DRM component can be added as an independent capability with automatic operation (e.g. sensitive documents found at the gateway in unencrypted form are automatically encrypted and registered with the IRM/DRM system according to pre-defined rules, with control of the documents handled independently via the outward-facing permissioning server).

- The functionality of the IRM/DRM component can be integrated into the DLP system (e.g. sensitive documents found at the gateway in unencrypted form are automatically encrypted and their usage managed by the outward-facing component of the DLP system, with a single reporting and audit system for both the DLP and IRM/DRM aspects of the system).

FileOpen provides a Developer Toolkit designed to enable tight integration of encryption and control functionality into existing applications and servers, and also provides complete systems that may be deployed alongside existing DLP systems with little or no direct integration.

A Proven Solution

FileOpen Systems is a leader in document security innovation and the mostly widely-used platform for controlled external publishing. With millions of secured documents in circulation, FileOpen has by far the largest footprint in the outbound publishing market. FileOpen Systems' extensive experience with publishing and extremely broad adoption of client software provides an unmatched platform for rapid deployment of IRM/DRM capabilities.

Unlike enterprise software, including DLP, where one company's internal systems may be entirely incompatible with another company's, publishing systems must be interoperable and use standard formats. Because no other system provides either the same degree of flexibility (granularity over client/server information flow and privacy, variable levels of security, native application support, etc.) nor the same breadth of openness and integration points, the FileOpen software represents the natural choice for integration by DLP vendors.