DOCAUTHORITY

White Paper

How To Succeed in Data Loss Prevention (DLP) Projects

Overview

Managing the abundance of sensitive information residing within an organization is extremely difficult. Mitigating the risks of a data leak is made harder by information that organizations cannot see, or even know to exist.

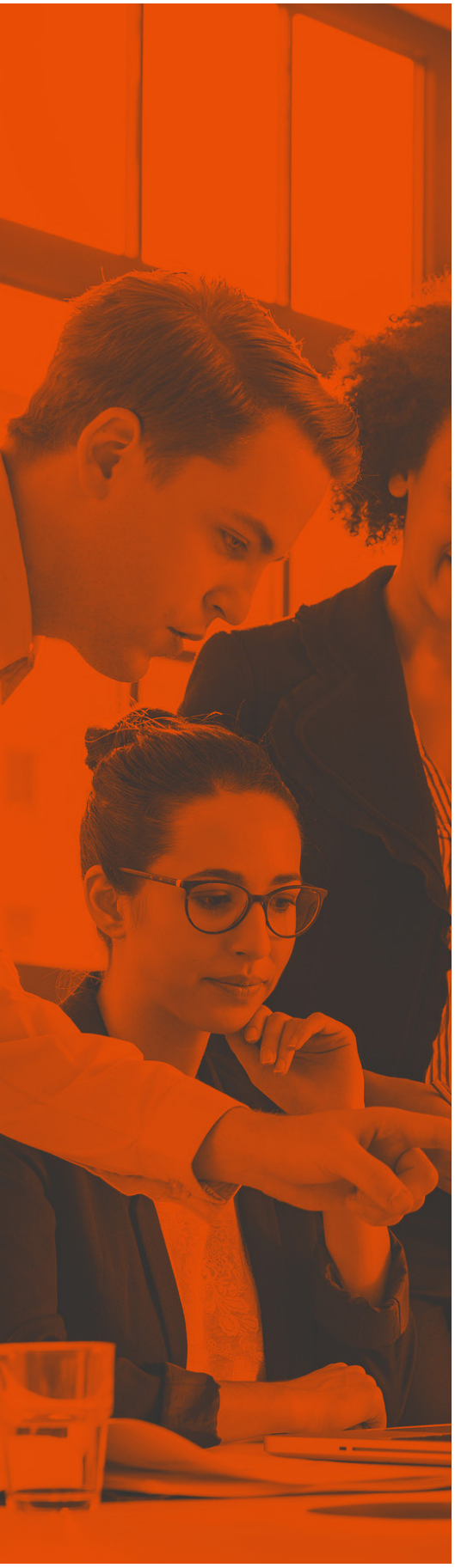
With intellectual property, customer data or business knowhow on the line, the damage of a data leak can be irreparable. The fallout can include loss of trust, regulatory fines, legal action, reputational damage and loss of business opportunities. Preventing this is not an easy fix. But that's where Data Loss Prevention (DLP) technology comes into play.

DLP technology aims to stem the leakage of sensitive data from within organizations. It does so by identifying data using textual rules and monitoring files and documents to secure the sharing of business data. It is a vital tool for organizations to get a handle on their sensitive information and significantly reduce the chances of data leakage.

Essentially, DLP is a powerful tool that helps you control where your sensitive data is going, making it a critical component in regulatory compliance and sensitive data protection programs.

How DLP Works

DLP projects can be a difficult burden to shoulder without understanding what data you have, and how it is used. It's impossible to keep up with the vast amounts of information that flows through an organization by manual processes alone. Here's how DLP can work to maximize the effectiveness of your data protection programs.



Text Rules

You can set content-specific rules that will identify a specific document through a combination of keywords. Unfortunately, it takes a significant effort to manually define and tune such rules per document, making scalability a considerable challenge. Furthermore, such rules usually aren't accurate and create a lot of false positives and impact business productivity.

Regular Expressions

Regular expressions are used to identify social security numbers, credit card numbers, passport numbers, national IDs, license plates and the like. By definition, regular expressions are mostly geared at privacy-related data and will not identify IP, commercial or other sensitive data. Furthermore, many types of privacy-related data will not be identified either, as they don't contain such identifiers (e.g. employee evals, recommendation letters). Regular expressions tend to create a significant number of false positives and productivity degradation.

Folders

DLP enables you to set a policy on a per folder basis. In reality, folders always have a mix of files with varying sensitivities and sharing policies. Setting distribution restrictions on a mixed folder will ultimately lead to incorrect blocking of data and business frustration and pushback.

DLP Success

Successful DLP implementations are based on the comprehensive coverage of sensitive data and a good sync between the DLP rules and how business users share the protected sensitive data. Unfortunately, many projects today are performed without an effective data discovery, identification and classification, and hence without knowing what the sensitive data is and who is its authorized recipients. Here are some of the consequences of this approach:

- Lack of knowledge of what is the sensitive data leads to very narrow DLP protection scope, thus to very limited value.
- DLP rules that are set without consideration to business data usage quickly disturb proper business processes and authorized data sharing, ending up in unreceptive business users and management, and some times in complete project cancellation.

Handling Sensitive Data

Below are four examples of sensitive data and its authorized usage:

- Final financial reports will be shared with management, the board and the stock exchange
- Board Meeting minutes will be shared with the board only
- Core IP will be limited to patent attorneys
- Management pension data will be limited to pension providers

How DocAuthority Helps

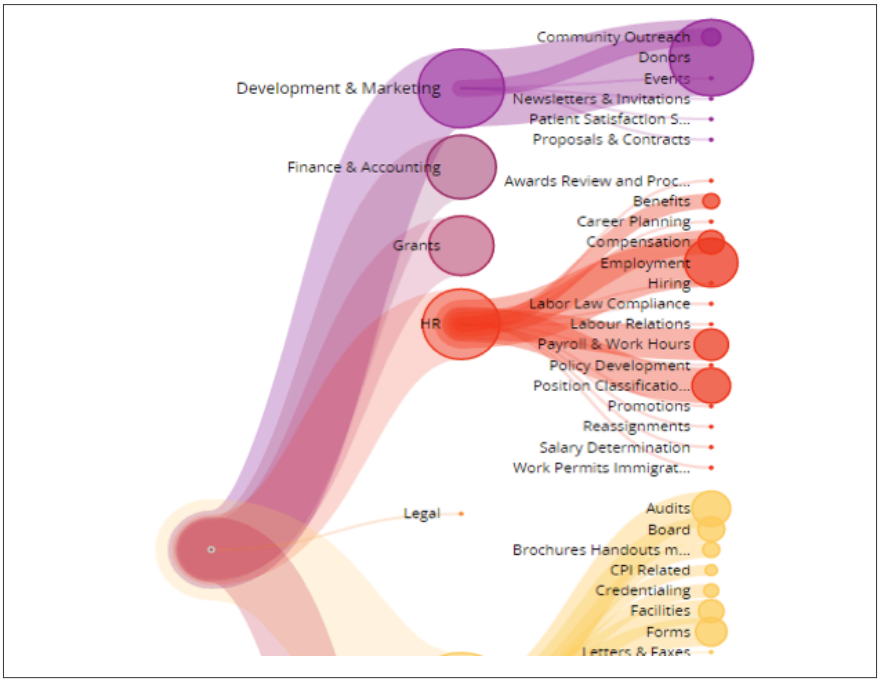
Using advanced AI technology, DocAuthority automatically identifies and categorizes data according to its business functionality, enabling you to define DLP policies per category. By building a data map, organizations are then able to apply data protection decisions that are tailored to specific busniess areas, taking into account their specific needs and data usage patterns. Using this apporach, both data is protected, and business productivity is not degraded.

DocAuthority's patented high-value technology eliminates the two biggest risks in DLP projects: Knowing what your sensitive data is and syncing DLP rules with authorized data sharing.

DocAuthority automatically and accurately discovers and identifies the business meaning of your data, enabling you to cover all of your sensitive data and easily align your DLP rules with its authorized use by the business.

What is the Build of Data?

Data is divided into business units / departments and carry specific functionality. For example, a file's category could be an Employment Agreement, Personnel Action Form, Invoice, Quote, Brochure or a Board Meeting Minutes. By making a business category-based policy decision, you set a policy that will be consistent across all files that conform to the same business usage. Furthermore, you can easily verify that your policy is aligned with how the business is sharing the files in this category, as the business now understands what the data is.



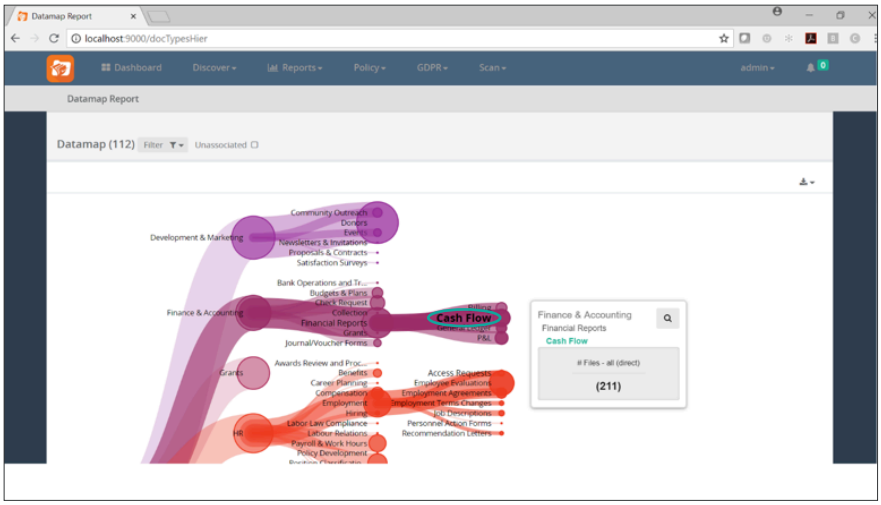
DocAuthority's Integration with DLP

DocAuthority integrates with most DLP solutions via file property tagging. In this method, a textual tag is physically embedded in a file's properties. In parallel, a rule would be defined in the DLP solution that if this tag is identified, a specific policy would be invoked. When this file is sent and analyzed by the DLP, the tag is identified, and the relevant policy is invoked.

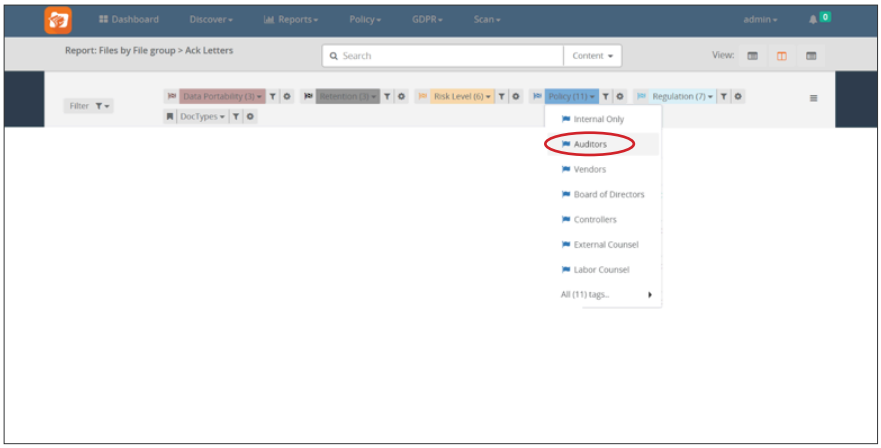
Example:

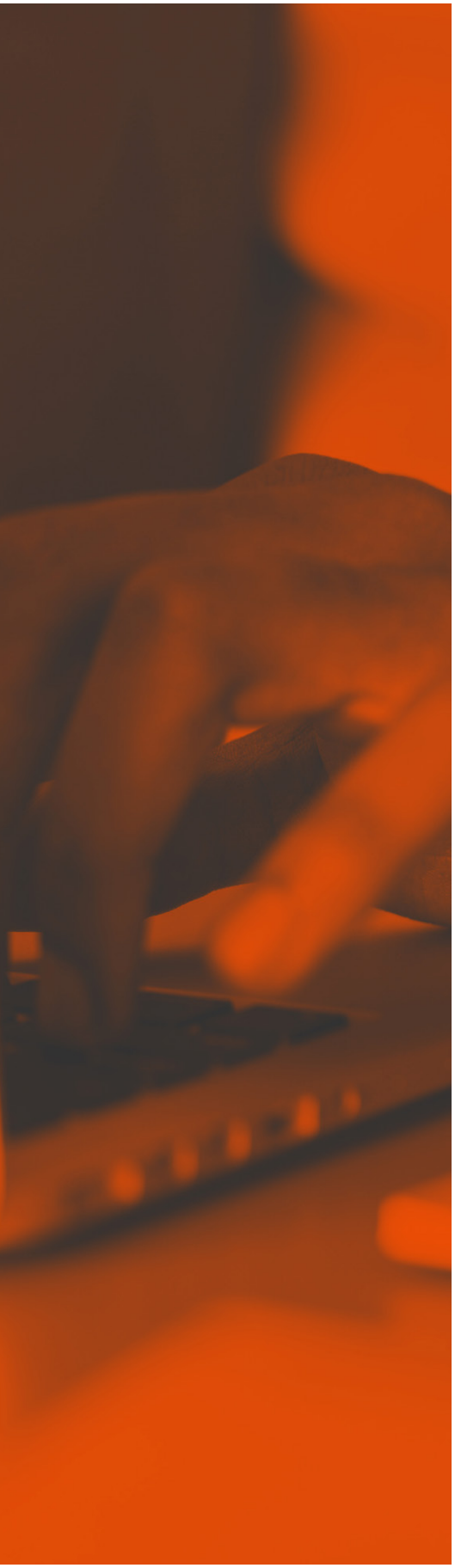
Step 1: A DLP policy is defined

Cash Flow category is selected:



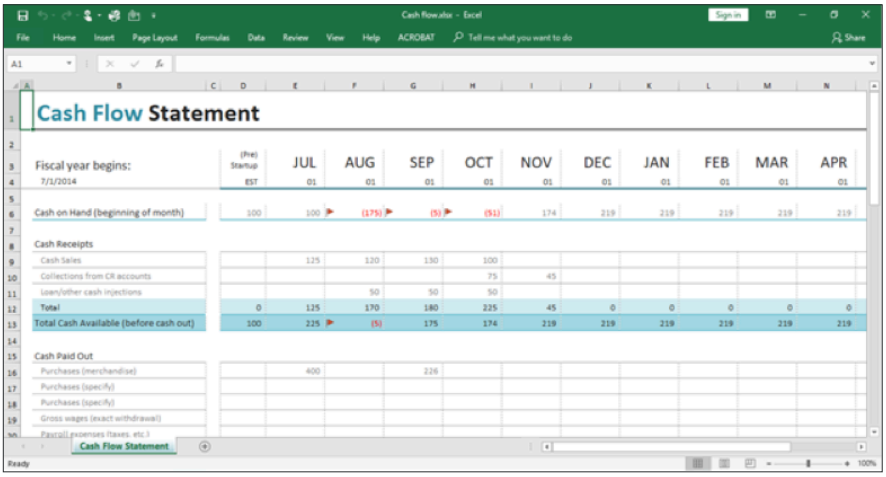
Select DLP policy:



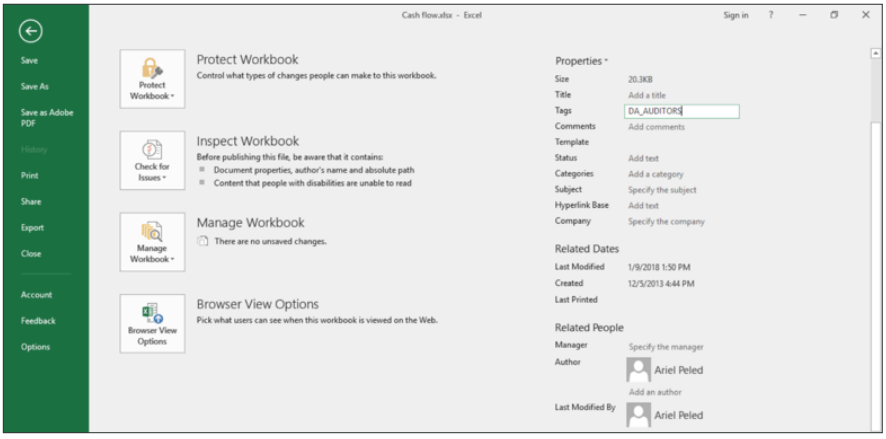


Step 2: A tag is embedded in a file

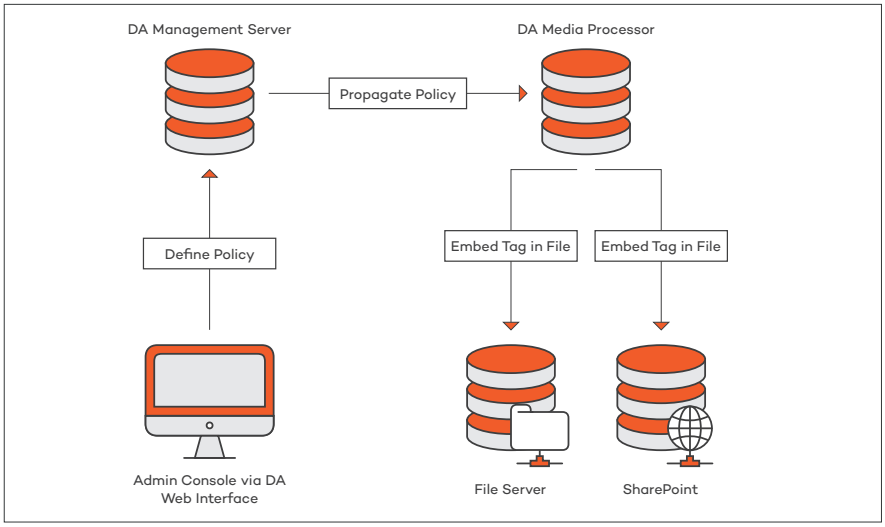
A cashflow document:



DA_AUDITORS policy is embedded in the properties area:

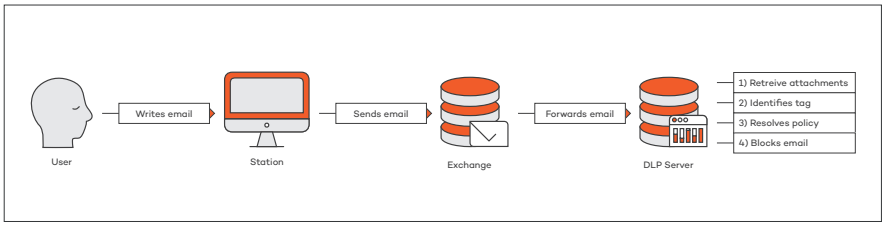


DocAuthority Tag Embedding Process:



Step 3: Policy is enforced

DLP tag identification and policy enforcement:



Conclusion

By combining DocAuthority with your DLP project you significantly improve the coverage of the data protected, the alignment of your rules with business's various data sharing patterns and thus the overall chances of the project's success.

DOCAUTHORITY

About Us

The explosion of data is a huge problem for organizations. Now with GDPR-like regulations coming into place, company data is now also a massive compliance risk. DocAuthority enables you to turn these compliance requirements into business opportunities and use them to dramatically improve all aspects of unstructured data usage, management and governance. DocAuthority's revolutionary and patented AI engine quickly and efficiently identifies and creates an inventory of all of your business data with the precision of 99.99%. With ease, you can now accurately identify both data's risk and its value and automate its ongoing classification, protection and retention while improving accessibility and quality.

Email

info@DocAuthority.com

Americas

+1 844 362-2884
3340 Peachtree Road,
Atlanta,
GA 30326

EMEA

+ 44 333 050 3241
Hamilton House,
Mabledon Place,
London
WC1H 9BB

APAC

+66 843 162 785
Sukhumvit Central
Business District,
51 Sukhumvit Road
Soi 8,
Klong Toey,
Bangkok
10110
Thailand

Israel

+972 1801 220 508
Ha-Tidhar St 15,
Ra'anana,
4365713
Israel