FORTRA™

SOLUTION BRIEF (Data Classification)

Fortra and Information Lifecycle Management

As unstructured data continues to grow, so do the places it may reside and hide. While document management repositories like SharePoint have made it easier to collect and manage unstructured data, the evolving methods of information sharing are making it impossible to capture all business records in one repository. Protecting and managing the lifecycle of an electronic document (and all of its copies) has exploded beyond the scope of just one solution. The ever-increasing usage of mobile devices, data sharing apps and services, and huge cloud data stores have intensified an already difficult problem. The future of information governance requires a new set of tools to manage information no matter where it resides.

The starting point for all data management and protection initiatives is to properly identify and classify your data. Industry analysts firms such as Forrester note that, "understanding and knowing your data is the foundation for both data security and privacy."[1] Unless you know what your data is, where it is, and why you are keeping it, it is impossible to enforce effective protection and compliance policies or manage the data's lifecycle.

BENEFITS OF FORTRA'S DATA CLASSIFICATION SUITE (DCS)

- Identify data value
- Optimize data management
- Enable defensible deletion
- Enhance eDiscovery
- Prevent data loss
- Analyze data sensitivity, access, and use
- Meet compliance requirements

Mobile sharing requires new tools to address the weaknesses of a centralized electronic document repository – namely that many important records aren't added to the corporate library due to user resistance and/or a lack of direct integration with the repository. To successfully manage information stored in multiple locations requires an increased focus on data identity and classification. Thoroughly knowing your data and where it is located are crucial requirements for proper records management in a decentralized world. As the focus shifts from containment to management, data identity enables the application of data protection strategies, retention management, and enhanced analytics for the information that resides outside of corporate document repositories.

Identification of data should begin immediately when the file is created to ensure the identity is not lost when the file is shared or moved. Identifying attributes, such as the classification, are applied by Fortra's Data Classification Suite (DCS) as persistent classification metadata. By embedding the identity as persistent metadata, users, security policies, and records management systems will have instructions on how to manage and protect the data, even when it is shared beyond the traditional data perimeter.

DCS can automatically apply classification metadata to information generated by line of business systems, downloaded from the web, or generated by users.

[1] Rethinking Data Discovery And Data Classification Strategies. by Heidi Shey and John Kindervag, March 25, 2016

DCS can illuminate your existing catalogue of unstructured data to discover, identify, and classify your legacy data.

Automated classification policy can be set based on static attributes, such as the source of the information and the folder location where the information is stored, or based on contextual attributes, such as file content. In cases where accurate automated classification may be challenging (for example, with business strategy or intellectual property documents), users can be guided in the manual application of the classification with easy to use toolbar buttons and pop-ups. To assist users with manual classification, system suggested classifications can also be provided to the user when making their selection. Regardless of the method used, it is necessary to properly identify the unstructured data—either by the system or the user—as something disposable or valuable.

DCS makes it possible to compare the data's identity with the recipient's identity to enforce secure data sharing policies.

In addition to creating processes for identifying data as it is created, DCS can illuminate your existing catalogue of unstructured data to discover, identify, and classify your legacy data. Information stored in network file shares, SharePoint, and Cloud repositories such as SharePoint Online, OneDrive, Box, and Dropbox can all be scanned to determine where sensitive data resides. By analyzing the content, context, and file properties, DCS is able to assign an identity to the file and apply persistent classification metadata.

The identifying information applied by DCS does not need be limited exclusively to the data's sensitivity. Virtually any other important attributes about the file—or about how the file should be managed—can be applied to the metadata. As the classification is being applied, DCS can also write to the metadata the appropriate compliance and retention codes. As a result, even if the data resides outside of an electronic document management solution (EDMS) this extra identifying information helps to ensure that data is easy to locate and that it is protected and handled according to government, industry and corporate requirements.

During its lifecycle, your organization's data will be accessed and shared with multiple users, so it is important that it is shared in accordance with policy. As a document makes its way through a workflow, the classification can be augmented to include the document status, such as "Draft", "Pending Review" or "Published". Based on the documents' status and sensitivity, DCS can be configured to automatically move sensitive files it finds in inappropriate or unsecured locations to secure folders, thereby helping to ensure access is restricted to authorized users only. When used in conjunction with SharePoint/ SharePoint Online, status and classification updates can also be used to manage user access and rights.

DCS can illuminate your existing catalogue of unstructured data to discover, identify, and classify your legacy data.

DCS email policies help to ensure that information and email attachments are only sent to the appropriate people. For example, organizations such as banks and investment firms may require "ethical walls" which prohibit the sharing of information between some groups of people within the same organization. By evaluating the sender, attachment, and recipient attributes, DCS can control the flow of information according to policy. In other words, DCS makes it possible to compare the data's identity with the recipient's identity to enforce secure data sharing policies.

Additionally, DCS classification metadata empowers the entire data governance ecosystem. As DCS performs a system-wide scan it can trigger your encryption or enterprise rights management (ERM) solution to immediately protect sensitive files where they are found. Data loss prevention (DLP) systems and cloud access security brokers (CASB) also benefit from the classification metadata. By reading the DCS metadata, DLP and CASB solutions are provided with the data's precise sensitivity and identity, empowering them to operate with increased accuracy. Downstream security technologies are no longer dependent exclusively on their own evaluation of the data but can rely on the DCS metadata (or a combination of the two) in order to make more accurate and fine grained policy decisions concerning the movement of information across the network or up to the cloud.

As data ages, it shifts from corporate asset to liability. It is advisable to delete data as soon as business and legal requirements allow, not simply to save money on the storage and eDiscovery costs associated with huge data libraries, but because this data may prove harmful in the event of a lawsuit. By adding identity and retention information to email and documents, it is possible for your archiving and records management system to make accurate decisions on what data should be kept, and what can be destroyed. An accurate and consistently enforceable retention policy provides your organization with a defensible position if challenged as to why information was deleted. In the event that you do need to locate information for audit, legal, compliance and regulatory requests, DCS metadata facilitates eDiscovery efforts.

In fact, DCS reporting capabilities make it much simpler to apply order to your information. The data captured in the DCS logs help security and records management personnel identify where data is, its sensitivity, and who has access. By analyzing data from the DCS logs, either in the native DCS dashboard or via your preferred business intelligence (BI) tool, records managers can target data requiring action, be that adding classification, moving the file to a secure location or archive, protecting the data with encryption, de-duplicating, or deleting expired records.

FORTRA'S DATA CLASSIFICATION SUITE (DCS)

Fortra's DCS for Outlook is an easy-to-use email security solution that ensures every Microsoft Outlook email's business value is identified before it is sent.

DCS for Microsoft Office is a security and document governance solution that ensures all Microsoft Office files are classified and protectively marked for security and compliance.

DCS for Desktop enables the classification and identification of any file type in a Microsoft Windows environment.

DCS for Data at Rest identifies, classifies, and protects data in network file shares and in the cloud, and provides analytics for insight into your data.

Fortra's Mail for iOS is an easy to use email and document security solution for mobile devices that prevents data loss and ensures the right users have access to the right information.

In addition to locating risks associated with the data itself, DCS can reveal a great deal about how your users are interacting with your sensitive documents. Integrated directly into popular business applications, DCS is able to report on actions users take with the most sensitive files. Policy alert reports help to identify groups or individual users who are struggling with corporate security policy and may require additional training. DCS reports can also be used to detect anomalies, such as multiple document classification downgrades in a short time, which might indicate a user has malevolent intent. By analyzing log data captured by DCS, it is possible to locate and correct a multitude of potential risks to the integrity of your information libraries.

DCS provides additional dimension to your data, making it easier to protect and manage the information lifecycle in accordance to policy in an ever decentralizing digital business world. The application of classification and other identifying metadata helps users and security systems recognize and manage information in accordance with policy. By classifying and identifying data as it is created, and across your existing data libraries on premise and in the Cloud, DCS solutions provide the necessary foundation of progressive information governance.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.