VERSION 1 • APRIL 2022

FILEORBIS' GOVERNANCE CAPABILITIES AND DATA STORAGE POLICIES

Overview: Content Analysis and Management Vision

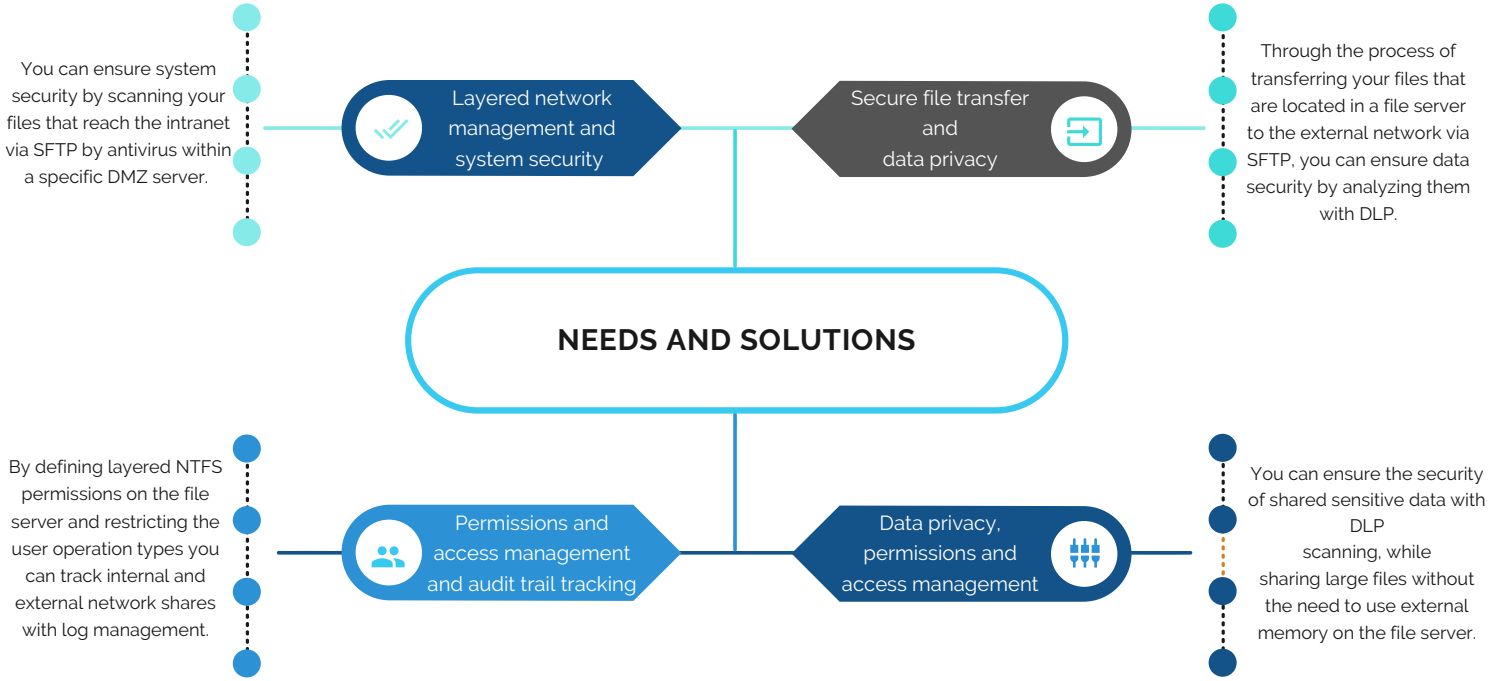
Nowadays, companies are increasingly becoming vulnerable to data loss as well as data leaks that can damage a company's reputation and disrupt daily operations. Data loss and data leaks can be prevented using FileOrbis' governance capabilities and data storage policies. Data leaks may not only be caused by hacking incidents. In fact, most data breaches can be caused by unintentional or malicious actions by employees for many reasons. FileOrbis' content analysis and management capabilities aim to minimize the risk of data loss for organizations against all unintentional and malicious actions.

FileOrbis Content Analysis Vision & Requirements

FileOrbis offers corporates data control to comply with security policies. The storage policy helps administrators automate data protection processes and secure and manage digital content. With increasing regulatory and business processes complexity, any misuse of files increases the risk of facing significant financial penalties while affecting the corporate's reputation. FileOrbis simplifies data management by setting policies for automatic document life-cycle management, including file aging and tracking of document movements.

FileOrbis Data Management Features:

- Content Scanning
- Data Discovery
- User Label / User Tag / Auto Tag
- Enforcement
- File Aging
- Warning Message Approval
- Reporting



FileOrbis Data Management Capabilities;

Content Scanning:

FileOrbis is based on a fast-indexing algorithm, which is used within content scanning as a layer of "pre-processing". All text-based files, PDF, MS Office, etc. are indexed by FileOrbis' analysis algorithm. With this index, FileOrbis allows users to search for content quickly, as is the search for similar word roots in the content. It can separate word roots in Turkish and English and expand the content search. Content scanning also parses the permission of the user that runs a search and can search all environments integrated with the system. You can also run analysis in e-mail attachments, file servers, integrated object storage, and MS Sharepoint with in-text features provided within MS Sharepoint. This way, the user cannot see results in locations that s/he is not authorized when searching extensively through all file environments. You can narrow the relevant in-text search properties based on many options such as language, metadata, location, and author by specifying filters.

Data Discovery:

With the FileOrbis content analysis service, files can be analyzed whether there is sensitive data in them or not by scanning while they are uploaded to the system or synchronizing previously integrated shared locations. Content Analysis Service(CAS), which can distinguish dozens of different data types and even verify some of them with verification algorithms, also offers custom regex support. CAS, which performs sensitive data analysis within files without DLP integration, can also analyze image-based files with OCR support. The types of data analyzed by the CAS service are increasing day by day. FileOrbis can verify phone, e-mail, etc. contents with format definitions. In addition, national IDs, credit cards, etc. data can be verified with the verification algorithm of the sensitive data. In this way, the number of "false positives" is significantly reduced.

.

User Label / User Tag / Auto Tag:
Files detected by CAS are automatically tagged. Files that receive tags based on the specified number and type of sensitive data form the basis of the sensitive data report. With this tagging, you can report where and what kind of sensitive data you have centrally. CAS can set and add automatic tags, as well as enforce users to add tags. Each user can choose from predefined tags and add user labels. In addition, as FileOrbis offers the features of tagging solutions, users are diversely given the possibility to add a "label" on files as they like. Thus, users can add keywords for their own needs in addition to the tags that are presented centrally, and they add filters by using these labels and quickly accessing their files.

Enforcement:
FileOrbis can apply enforcement like blocking on actions triggered on security and other rule layers as the action of specified policy. This action can also be applied to results triggered by external DLP solution integration. In addition, you can make tag-based enforcement for files tagged by FileOrbis CAS. These controls can be defined as blocking downloading, blocking uploading, blocking linking, and blocking sharing. If there is sensitive data, you can automatically do these controls through FileOrbis based on a rule. FileOrbis can also perform non-blocking actions. If a file containing sensitive data is tried to be shared with internal users or is tried to be sent to an external party, an approval flow can be enforced. Based on the flow, people receiving approval requests can analyze the details of requests, and it can be ensured that sensitive data is accessed only under approved conditions.

File Aging:
Files on FileOrbis can be aged based on the date of the last read, write, and edit. You can make the user and file path-based exceptions on FileOrbis, which can apply aging as deletion or move to another location. It is also possible to age according to sensitive data content. In this way, you can prevent sensitive data from creating risks by being unnecessary in user access and can control costs by controlling the size of your file environments.

Warning Message Approval:

With FileOrbis warning message approval, you can create a link with warning message approval which forces external users to approve the presented warning message before getting access to files and folders shared with them. In this way, access to documents containing critical data that is obliged to protect depending on regulation is gained with the "read, approved" consent of the external users. All approvals are also kept as logs in the reports and are stored for use in the necessary legal proceedings.

Reporting:

FileOrbis records 150+ operations of the system administrator and users with many parameters such as user, process, file, IP, browser, OS, interaction. FileOrbis parses all operations and internal fractures, keeping a lot of detail and allowing you to form different alarm mechanisms through these details. The logging mechanism, which can also be supported with SIEM integration, is also offered to the system administrator with an easily readable interface. You can view the main operation log and log detail as needed and narrow your queries with contact, process, date filters. You can also download the results that you will achieve with the relevant filters as MS Excel files at that time or even have these results automatically sent in certain intervals in the report form.

Figure 1a: Critical Data Scanning

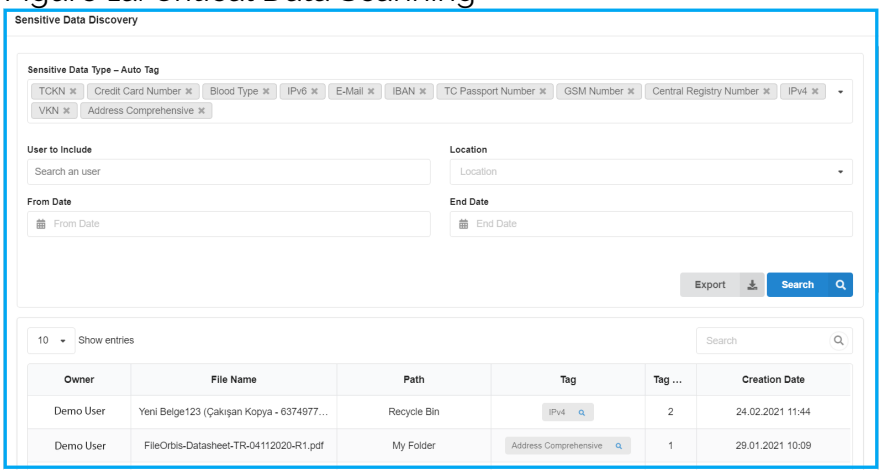


Figure 1b: Reporting