FileFacets Product Overview

FileFacets Product Overview

While today's Enterprise Content Management (ECM) systems are built to organize data for records management and file sharing, the onus of evaluating and processing billions of files is a daunting task for any corporation. For businesses migrating large amounts of data from one or multiple systems to another, the discovery, classification and attribution of content with relevant business value can take months or even years.

FileFacets' cloud data analytics and content migration platform makes it easy for businesses to manage and migrate data by automating the categorization of data, the attribution of file metadata and the migration of unstructured content from multiple sources into structured ECMs.

FileFacets' automatic file sorting algorithms make it simple for organizations to locate essential data. The solution can access and scan files without interruption and detect duplicate files before moving them. Additionally, FileFacets analyzes and leverages file metadata, as opposed to actual content, so an organization's data remains secure.

As the only migration tool available as a pure SaaS solution, it is able to easily scale and support a number of users across multiple locations in a safe manner.

FileFacets addresses the need of all Information Governance (IG) professionals to establish and maintain control of enterprise-wide records. FileFacets is designed to support all IG policies and processes with modules that:

- remove ROT (Redundant, Obsolete & Trivial) files
- isolate duplicates
- attribute metadata
- build out target taxonomies
- facilitate auto-classification of content
- migrate data to numerous platforms or repositories.

FileFacets migrates unstructured content from multiple sources into Enterprise Content Management (ECM) systems, facilitating ROT processing (Redundant, Obsolete & Trivial files), auto classification, taxonomy implementation, and metadata mining and attribution.

Saves Time

By automating the process of categorization and file attribution, FileFacets can save weeks, months, even years of manual file categorization, attribution of metadata and content migration.

Increases Productivity

Because FileFacets runs in the cloud and does not interfere with source content organizations Uninterrupted workflow, business units and users continue to work as usual.

Flexible & Scalable

FileFacets online environment makes it both easy to deploy and cost effective to implement, effortlessly scaling to support an unlimited number of users across multiple locations.

Safe & Secure

While FileFacets collects the properties and attributes of the files for processing, all source content remains secure in its native repositories, keeping all sensitive data secure.

FileFacets Make Data Management & Migration Easy with a Single Tool for:

Data Analytics:

- Content Analytics & Project Design
- Content Classification including Dynamic Clustering
- Metadata Extraction & Attribution
- Redundant, Obsolete, Trivial (ROT) Processing & Deduplication
- Personally Identifiable Information (PII) Processing
- Audit capability to support Quality Control

Content Migration:

- Taxonomy Builder
- Pre-migration staging area to view target state and repositories
- Collaboration and approvals within the application itself
- Capture from, and migration to, multiple repositories
- Metadata is in the cloud, files move directly from source to target

We make it easy for businesses to manage and migrate content.

Product Features

Features	Benefit	Why
Hybrid-cloud Environment	Secure	Content stays secure in source repositories - only the metadata, properties and attributes are stored in the cloud
Dashboard	Smart Decision Making	Real time analytics on file attributes, project phases, duplicates, storage and location
ROT Processing	Saves Money	Excludes all Redundant, Obsolete, Trivial (ROT), including duplicates to focus on Business-Value Content only
Data Identification & Security	Maintains Privacy	Identifies Personally Identifiable Information (PII) and keeps PII data secure
Auto-Categorization	Saves time	Save months of manual file migration, categorization, attribution
Metadata Mining & Attribution	Saves Time	Collect properties/attributes of the files and restructures source content using a target staging area
Content Migration	Increases accuracy	Enables you to design, solicit buy-in, and test before committing to deployment
Audit Capability	Quality Control	Audit capability shows content structures and history

System Performance

There is no limitation on concurrently deployed agents and no performance degradation as volumes increase. This performance baseline was determined using 5 Virtual Machines running 1 agent per CPU. To further reduce the processing time, simply add VMs and concurrently deployed agents.

Scan Speed of 100M files

- Metadata scan – 40 hours
- Full Content – 150 hours

Scanning includes:

- ROT Processing
- Deduplication file count
- File age
- File size
- File type
- File location
- File Dates

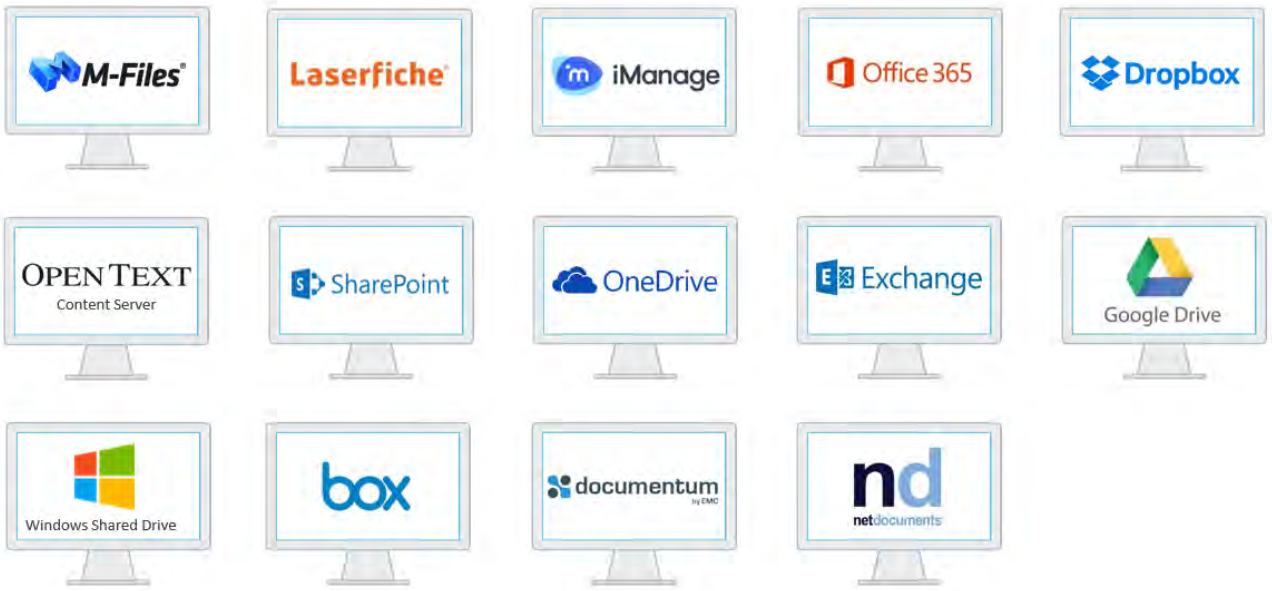
System Requirements

FileFacets is a hybrid cloud solution with a File Access Agent installed in the customer environment. The specifications for using the agent are below.

Operating System	Windows Server 2008 R2 or higher
CPU	Quad Core minimum
RAM	8 GB minimum
Storage	5 GB minimum
Installed Software	.NET 4.5 framework Microsoft Office IFilter components
Browser	IE10+ / Chrome / Firefox

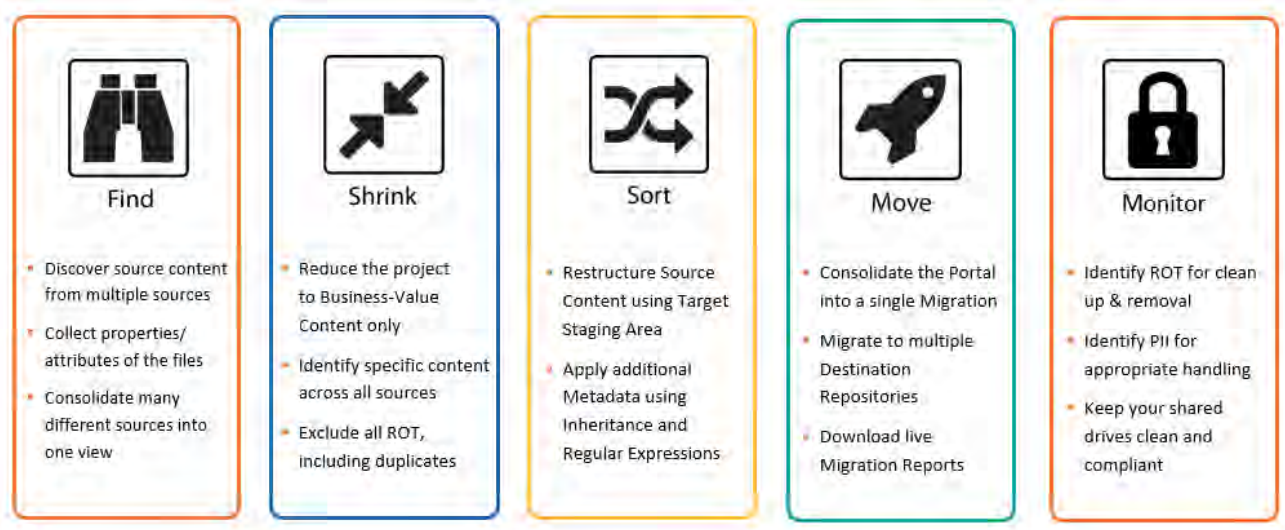
ECM Connectors

FileFacets migrated from and into the following ECM and file sharing technologies.



FileFacets Methodology

FileFacets features a five-step methodology for successful data analytics and content migration.



Capturing Data

In this phase, users gather the information they wish to categorize by defining Capture Sources, Creating Segments to segregate folders for rule based ROT processing, and view Content Analysis Reports that show an overview of the content found. The Capture Report contains valuable information that can help identify the sources of some of the ROT that might currently exist within an organization.

File Clean-up

Most file repositories contain a large number of files without any valid business value. These may be duplicates, out of scope, or deemed as otherwise trivial. In this phase, the user can create rules to identify these files and process them accordingly. This could mean that they will not be migrated, or archived to a separate destination, or simply flagged for deletion. Redundant, Obsolete, and Trivial files clutter your record repository ad cause the structure to become increasingly difficult to manage. Finding those records and managing them is simple with the Shrink module of FileFacets.

Content Design

In the Content Design module, the user can create the Target Structure, create and assign Metadata Elements and Metadata Groups, and list valid Metadata Values with which to tag the files. Additionally, the user can create and apply Retention Schedules to Target folder structure.

Classification

In this section, source files are mapped to the target structure using a "drag and drop" method. The user can map individual files or groups of files using standard actions, and add folders and subfolders to the existing structure in the same wad this was accomplished in the Content Design module. To aid the mapping process, the source can me filtered to Show All Files, Show Mapped Files, or Show unmapped files. Any system metadata captured with a file is also shown on the Show Source Metadata face.

Clustering

The Clustering feature of FileFacets allows the user to group the files based on their content. Using the Clustify™ engine, the user can build a model that will create clusters based on subject matter or common passages of text, for example, finding all saved emails in a thread and keep them together.

Regular Expression

The Regular Expression features of FileFacets allows the user to extract metadata from the file contents. Using these Regular Expressions, the user can define specific string formats, or lists of keywords needed to apply to the files in other ways. This feature includes the ability to apply the extracted values as folders.

PII/PIHI Processing

Using the Regular Expression feature within FileFacets, the user can search for and segment any Personally Identifiable (PII) data, such as Social Security Numbers, Driver's License number, and credit card information. These files are flagged so the user can quickly identify which files contain this sensitive information to enable the user to handle or process appropriately.

Project Audit

Now that the mapping is complete, and all the records are in a target location assigned, the user can run a disposition report that will allow their team to review the files that have met their retention and decide if they can be disposed of. The user can download an excel spreadsheet that will facilitate the review process.

Pre-Migration

The Pre-Migration function provides a number of features for preparing files to be migrated to the target system. In this section, the user can find and replace the file names to follow a prescribed style guide or convention. In the Special Character section the user can replace ineligible characters to ensure a successful migration into ECM.

Migration

Similar to the Capture function, the Migration functions use the interface within FileFacets to send instructions to the Capture and Migrate Utility installed on the network environment. A Migration can be initiated from the Start Migration section, beginning the process of moving files as defined by the project. This includes file cleanup, file mapping and attribution, file renaming, etc. the Migration function reports back on the status of the Migration upon completion showing any files which could not be migrated, and may require manual analysis and intervention. The migration process is run using a script that provides the location where every file mapped from the source to the target is directed to go in the new repository.

FileFacets Security

Information Security	
General Information FileFacets maintains a Security Officer certified under the Industrial Security Program as mandated by the Federal Government. The program policy and standards cover the requirements for any staff dealing with any classified information, assets or workplaces belonging to the Federal Government. The Security Officer is qualified to make decisions regarding security matters; has authority to enforce compliance; these eligibilities are based o their certified knowledge of security principles and practices. Areas of expertise comprise (but are not limited to): Handling and Safeguarding Information including storage, transportation and destruction; Developing and implementing security plans, including Performing Threat and Risk assessments, assessing and advising of physical controls; advising on and reviewing personnel screening activities for all staff that come in contact with any client data. All FileFacets individuals are screened under this standard.	
Does FileFacets have documented security policies and standards?	Yes
Does FileFacets have established specific policies, processes and procedures to safeguard client data?	Yes
Are security policies reviewed by Management at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy?	Yes
Has the FileFacets hosting provider completed a SSAE 16 assessment? If yes, what scope or sections?	Yes, Azure had this assessment SOC1 and SOC2
Are other independent reviews, assessments and/or audits performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements?	LunarLine penetration test

Privacy	
Does FileFacets maintain information privacy policies, standards, guidelines and controls in place to prevent unauthorized access or misuse of confidential information?	Yes
Does FileFacets knowingly and actively collect private information?	No
Do FileFacets staff sign Non-Disclosure agreements at time of hire, and are these NDAs reviewed on an annual basis?	Yes
Does FileFacets maintain and enforce an IT Acceptable Use Policy that clearly outlines practices staff are allowed to follow with corporate physical and information assets?	Yes
Data Security	
Is the network transfer to client data encrypted when traversing to the FileFacets network	Yes
Is all network transfer of client data encrypted between multiple FileFacets systems and within their network? (e.g. between web, application and database servers)?	Yes
Does FileFacets support and offer encryption for data at rest (databases)?	Yes
What is the encryption algorithm and key strength user?	AES 256 – 32 random characters
Will any client data be stored, temporarily or otherwise, on end-user workstations, portable devices, or removable media?	No
Is client data encrypted in storage outside of database and live storage (e.g. backups to tape, Disk/file system, jump drives, etc.)?	Only location that data is stored outside of database is the encrypted back-up
How is the back-up data secured?	Database backups are stored by Azure
Is client data back-up data stored off-site?	Yes
Is the activity of FileFacets technical staff logged when performing system maintenance?	Yes
Network Security	
Is client data hosted by FileFacets accessible over the Internet (rather than or in addition to a private connection)?	Yes
Can access to client data hosted by FileFacets be controlled by the source IPs or similar mechanisms?	Yes
Is the FileFacets application or data transmission process proxy compatible?	No
Will client data hosted by FileFacets be accessible from mobile devices?	No
Does FileFacets perform network penetration testing either themselves or by a contracted outside firm? If so, how often?	Yes, annually.
Are Security logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events retained?	Yes
How frequently are security logs reviewed?	Daily
Is physical and logical user access to audit logs restricted to authorized personnel only?	Yes
Operational Controls	
Does FileFacets outsource hosting of their application and data storage services to a third-party?	Yes

Where is client data located?	All clients' information is stored at Microsoft Azure Hosting. The FileFacets portal (web interface) is also hosted by Microsoft Azure. Canadian companies have their information stored in Canadian Hosting, and U.S companies have their information stored in the U.S Hosting.
Has FileFacets taken measures to ensure the data center(s) in which client data is housed have controls for: 1. Controlled physical access and audited entry ways 2. Temperature/humidity monitoring and control 3. Fire prevention and suppression 4. Use of conditioned back-up power	Yes
Does FileFacets implement anti-malware controls on servers and staff workstations?	Yes
Does FileFacets outsource information destruction services?	Once FileFacets has designated what files are to be deleted, Microsoft will perform the actual data wipe where the files are stored. Only the files selected will be deleted.
What methods are used to ensure that FileFacets employees, who have access to client data, have been properly vetted? (e.g. law enforcement background checks)	All staff must undergo a background check by a Sterling BackCheck, a company that specializes in employee screening. The process established personnel screening standards to ensure that only persons whose reliability and trustworthiness have been established are granted access to protected information, assets, or sites. The application process reviews the applicants' background through: criminal records checks, identify cross checks, employment verifications, reference checks, and credit bureau inquiry with ID cross checks.
Application Security	
In the software development life-cycle does FileFacets incorporate features from any standards-based framework models?	Microsoft SDL
Are security components identified and represented during each phase of the software development life-cycle?	Yes
What software development platform does FileFacets use?	.NET
Does FileFacets perform application vulnerability scanning?	Yes. Development and Production environments are physically separated. Production and test are logically separated.
Are technical controls established to prevent unauthorized remote code from executing?	Yes