SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

How to clean up the file system

www.searchinform.com

Why is it important to classify and sort out confidential data? Why keep track of changes in the document content and keep an archive of edits? Is it possible to identify an insider by the files name on their PC? Let's take a look at real examples, which explain where to start monitoring data at rest.

IMPORTANT THEORY

When tracking the movement of corporate documents (read: data in motion), it is easy to forget about data at rest protection. Some DLP systems are able to detect on which servers and PCs confidential files are stored using the eDiscovery mechanism.

However, knowing that all price lists are located in the same folder is not enough to fully protect them. You need to find out which employees have access to it, as well as who opens and edits the confidential documents. For example, excel table "Employees" can store personal data of VIP clients, and the "Sort" folder can comprise of financial reports. The solution to all these issues is a DCAP.

DCAP systems (Data-Centric Audit and Protection) perform an automated audit of data in the file system, find access violations, and track changes in important documents. The system gives insight on how much valuable data the company has, where it is stored, which employees can use it and how they use it.

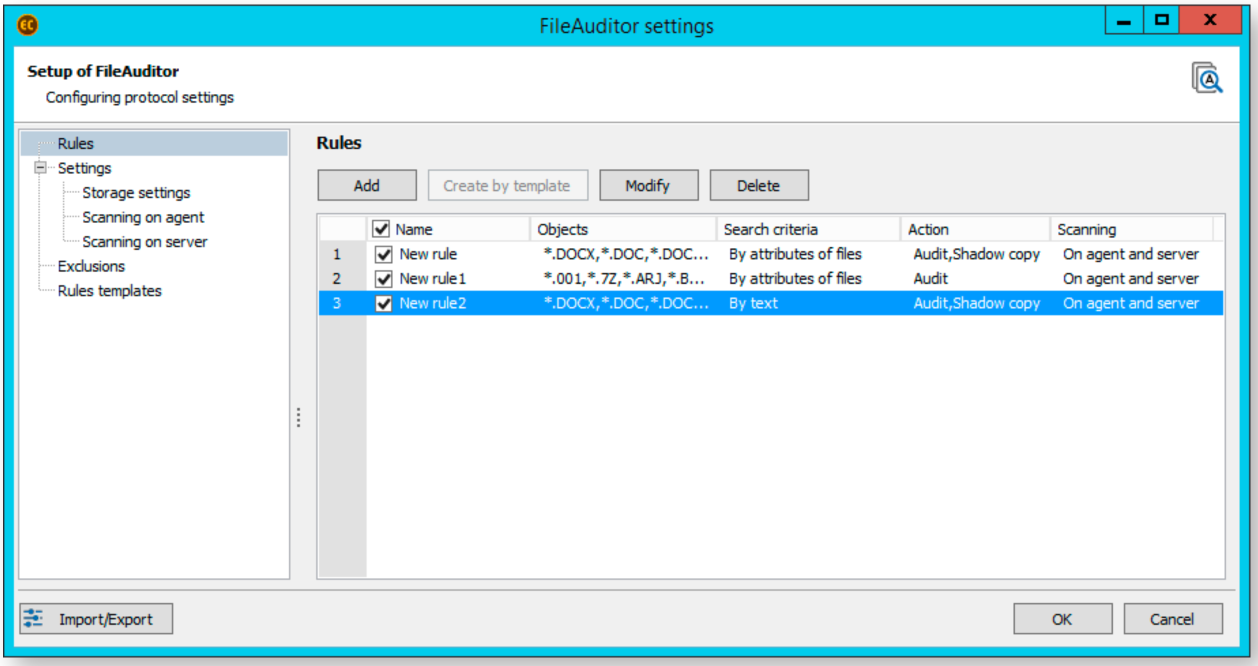
Now, let us get down practicing part! We are eager to share non-fictional customer stories based on SearchInform FileAuditor experience and show how DCAP systems solve customer problems.

PROTECTION AGAINST ACCIDENTAL DISCLOSURE

Case. It was revealed that in a shared network folder by negligence or mistake employees stored passport scans, later on, other personal data was found on PCs. Such confusion and carelessness in the documents can result a company into a GDPR fine or, what is certainly worse, into losing valuable information. Luckily, this case had no incidents. FileAuditor helped detect and fix the problem.

How does it work? DCAP systems essentially are search algorithms. The functionality of the solution depends on their quantity and quality. The more powerful the search engine, the more quickly and effectively the program will work.

FileAuditor now has four types of search – by text, regular expressions, attributes, and dictionaries. The configuration of data control policies enables you to set up search terms and select scan objects (file, storage location). For user convenience, the program has ready-made rule templates.



	☑ Name	Objects	Search criteria	Action	Scanning
1	☑ New rule	*.DOCX,*.DOC,*.DOC…	By attributes of files	Audit,Shadow copy	On agent and server
2	☑ New rule1	*.001,*.7Z,*.ARJ,*.B…	By attributes of files	Audit	On agent and server
3	☑ New rule2	*.DOCX,*.DOC,*.DOC…	By text	Audit,Shadow copy	On agent and server

Example of data control policies in FileAuditor

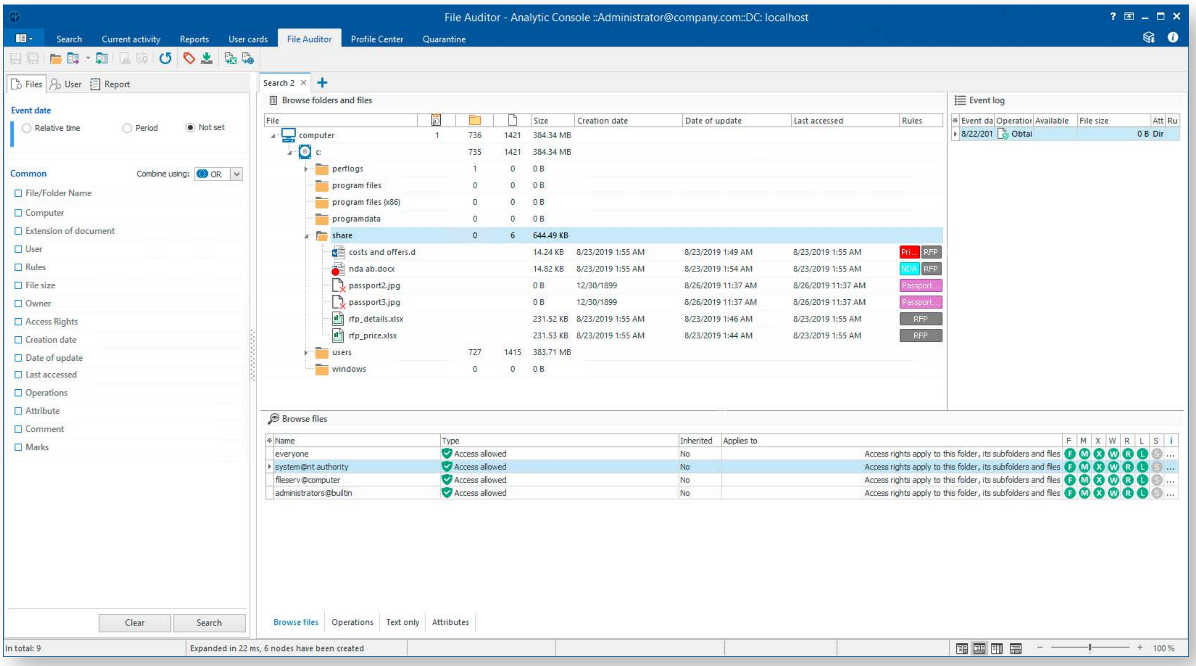
In fact, they classify documents by content. This way you can categorize all relevant information in the corporate network – "Office files", "Contracts", "Prices", "Personal data", etc. Then, the program makes scanning and, if the file falls under the policy, FileAuditor puts a "label" on it.

Scanning has two modes: server and agent based. You are very welcome to use both. Server based mode allows scanning data in network folders and on servers, whereas agent based mode enables files scanning on employees' PCs. You can configure the scanning schedule. More than this, the program will first scan edited and new files. By doing so, FileAuditor helps to identify an insider or a violator as soon as appears.

The scan results are collected in the Analytic console. Here you can see a tree of labeled folders with enclosed files into them (the label color could be set up according to tailored policies). Now all confidential documents are visible and you can take hold of them, as the company from the first case did.

The error report allows you to check the progress of the scan. It indicates the technical problems the program encountered while monitoring a specific file or folder. For example, the server where the file or folder were stored was not available.

Analytic Console also enables to track access rights to files and folders. The software analyzes configured permissions and displays them in the "Browse files" mode.



File				Size	Creation date	Date of update	Last accessed	Rules
computer	1	736	1421	384.34 MB				
c:		735	1421	384.34 MB				
perflogs		1	0	0 B				
program files		0	0	0 B				
program files (x86)		0	0	0 B				
programdata		0	0	0 B				
share		0	6	644.49 KB				
costs and offers.d				14.24 KB	8/23/2019 1:55 AM	8/23/2019 1:49 AM	8/23/2019 1:55 AM	Pri... RFP
nda ab.docx				14.82 KB	8/23/2019 1:55 AM	8/23/2019 1:54 AM	8/23/2019 1:55 AM	NDA RFP
passport2.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	8/26/2019 11:37 AM	Passport...
passport3.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	8/26/2019 11:37 AM	Passport...
rfp_details.xlsx				231.52 KB	8/23/2019 1:55 AM	8/23/2019 1:46 AM	8/23/2019 1:55 AM	RFP
rfp_price.xlsx				231.53 KB	8/23/2019 1:55 AM	8/23/2019 1:44 AM	8/23/2019 1:55 AM	RFP
users		727	1415	383.71 MB				
windows		0	0	0 B				

Event da	Operatior	Available	File size	Att	Ru
8/22/201	Obtai		0 B	Dir	

Name	Type	Inherited	Applies to	F	M	X	W	R	L	S	i
everyone	Access allowed	No	Access rights apply to this folder, its subfolders and files	F	M	X	W	R	L	S	...
system@nt authority	Access allowed	No	Access rights apply to this folder, its subfolders and files	F	M	X	W	R	L	S	...
fileserv@computer	Access allowed	No	Access rights apply to this folder, its subfolders and files	F	M	X	W	R	L	S	...
administrators@builtin	Access allowed	No	Access rights apply to this folder, its subfolders and files	F	M	X	W	R	L	S	...

In total: 9

Expanded in 22 ms, 6 nodes have been created

List of users with their access rights to the selected folder and files in it

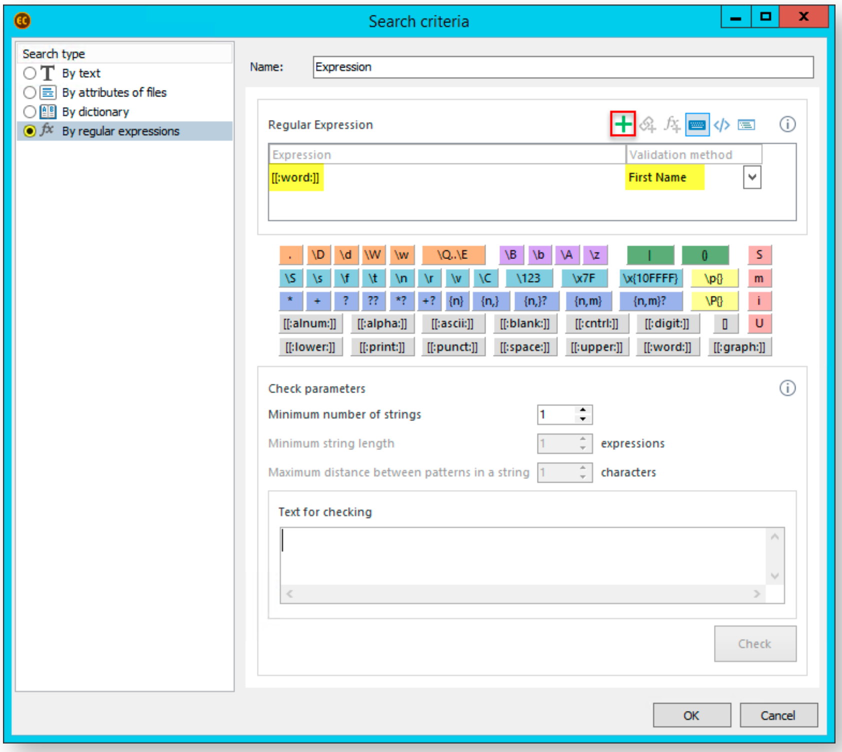
The file owner report is available in the Console and helps to understand who owns a document or folder. It simplifies tracking new objects in the file system.

What to monitor first?

Create a list of files that need to be kept under special control (files containing trade secrets, personal data, accounting documents, etc.). Make it as complete as possible.

Here are some recommendations for creating data control policies in FileAuditor:

1. Track documents with labels ("For official use", "Secret", "Commercial secret", etc.). Use text search based on morphology, by exact match, or by mask.
2. Monitor contracts, commercial offers, and agreements. Originals and versions can be easily found by the sequence of characters (Contract # 29\) or by the mask (contract.?,#*. docx).
3. Set up a search using regular expressions (mathematical "formulas") to monitor documents with personal data, namely, passport numbers, phone numbers, payment cards, etc.



Search criteria

Search type
○ By text
○ By attributes of files
○ By dictionary
● By regular expressions

Name: Expression

Regular Expression

Expression	Validation method
[[:word:]]	First Name

Check parameters

Minimum number of strings: 1

Minimum string length: 1 expressions

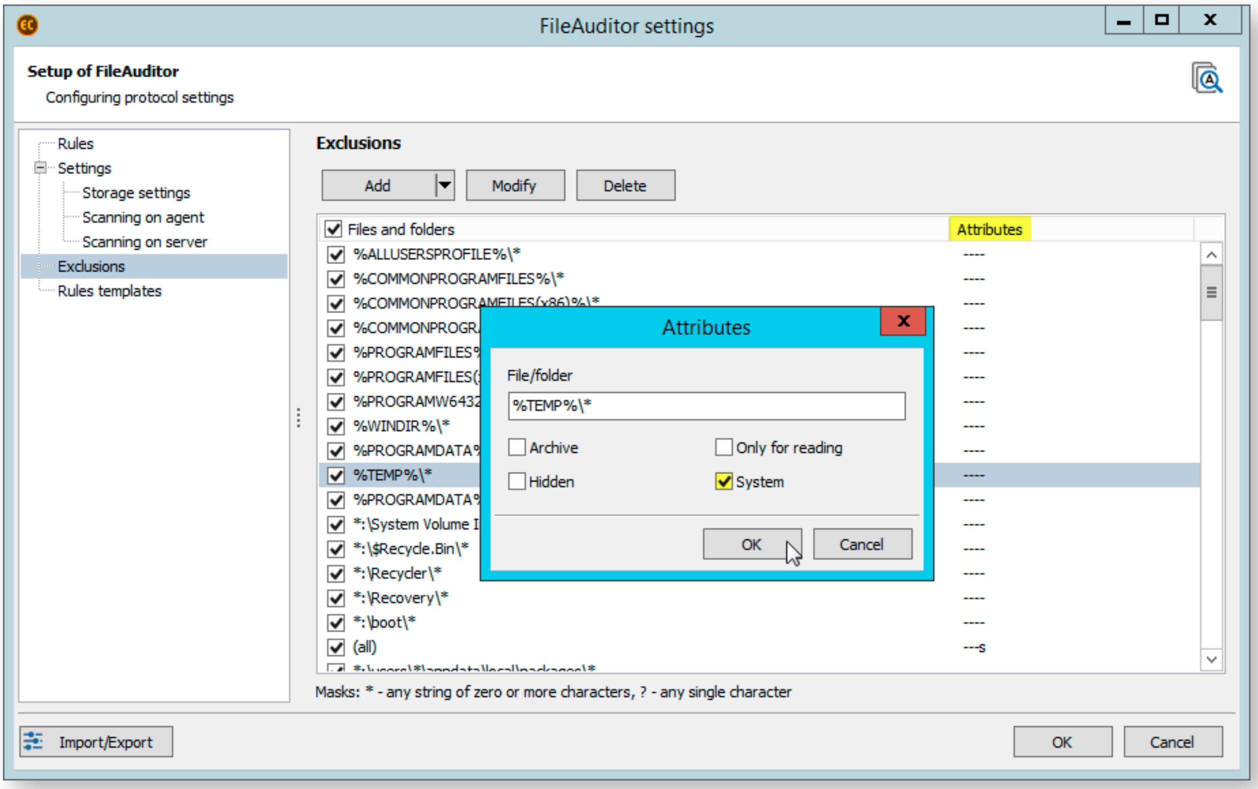
Maximum distance between patterns in a string: 1 characters

Text for checking

Configure regular expression search for documents that contain the payment card number

Some files and folders can be excluded from scanning to save time. For example, there is no need to spend software resources on analyzing system files.

FileAuditor enables you with flexible settings, where you can adjust the list of exclusions by category, extension, location, etc.



☑ Files and folders	Attributes
☑ %ALLUSERSPROFILE%*	----
☑ %COMMONPROGRAMFILES%*	----
☑ %COMMONPROGRAMFILES(x86)%*	----
☑ %COMMONPROGR	----
☑ %PROGRAMFILES%	----
☑ %PROGRAMFILES(	----
☑ %PROGRAMW6432	----
☑ %WINDIR%*	----
☑ %PROGRAMDATA%	----
☑ %TEMP%*	----
☑ %PROGRAMDATA%	----
☑ *:\System Volume I	----
☑ *:\$Recycle.Bin*	----
☑ *:\Recycler\*	----
☑ *:\Recovery\*	----
☑ *:\boot\*	----
☑ (all)	---s
☑ *:\users\*\appdata\local\packages\*	

Masks: * - any string of zero or more characters, ? - any single character

File/folder: %TEMP%*

☐ Archive ☐ Only for reading

☐ Hidden ☑ System

Add system files and folders to the exclusions

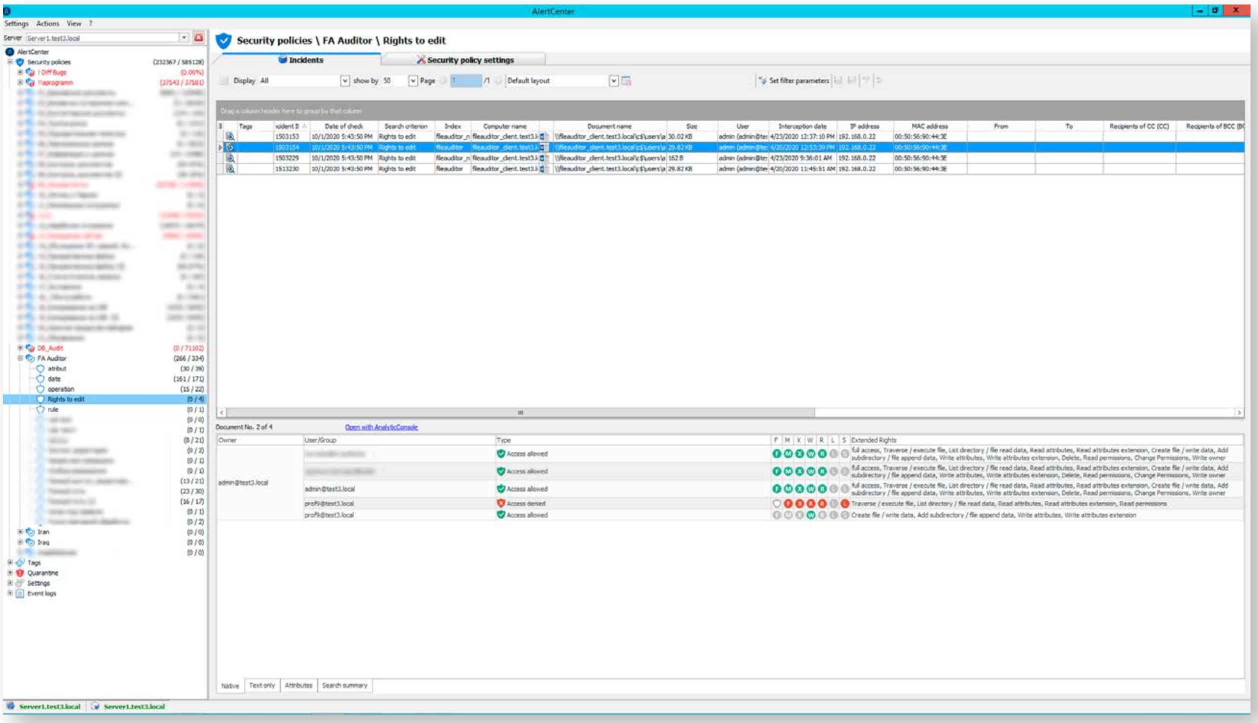
PREVENTING LEAKS

Case. Before dismissal, a retail company marketing specialist downloads an expensive market study from a file server to his PC. After a while, the downloaded file no longer falls into the "trade secret" category. Having received an alert from FileAuditor, a risk manager reviews the changes made to the document. The risk manager finds out that the employee shortened the document text and partially rewrote the content. The investigation revealed that the employee had an intention to pass off the research as his own to make a good impression on a future employer.

How does it work? FileAuditor displays all user actions with files in the "Operations" mode in Analytic console. This very option helped the security manager to restore the chronology of the employee's actions and collect evidence of a violation.

How not to miss an incident?

AlertCenter console helps to stay up to date by sending notifications about detected violations to an email. To track incidents effectively in a few clicks, you can enable notifications about new critical files or employees from risk groups working with them.



Tags	ncident ID	Date of check	Search criterion	Index	Computer name	Document name	Size	User	Interception date	IP address	MAC address	From	To	Recipients of CC (CC)	Recipients of BCC (B
	1503153	10/1/2020 5:43:50 PM	Rights to edit	fileauditor_n	fileauditor_client.test3.l	\\fileauditor_client.test3.local\c$\users\a	30.02 KB	admin (admin@te:	4/23/2020 12:37:10 PM	192.168.0.22	00:50:56:90:44:3E				
	1503154	10/1/2020 5:43:50 PM	Rights to edit	fileauditor	fileauditor_client.test3.l	\\fileauditor_client.test3.local\c$\users\a	29.82 KB	admin (admin@te:	4/20/2020 12:53:39 PM	192.168.0.22	00:50:56:90:44:3E				
	1503229	10/1/2020 5:43:50 PM	Rights to edit	fileauditor_n	fileauditor_client.test3.l	\\fileauditor_client.test3.local\c$\users\a	162 B	admin (admin@te:	4/23/2020 9:36:01 AM	192.168.0.22	00:50:56:90:44:3E				
	1513230	10/1/2020 5:43:50 PM	Rights to edit	fileauditor	fileauditor_client.test3.l	\\fileauditor_client.test3.local\c$\users\a	29.82 KB	admin (admin@te:	4/20/2020 11:45:51 AM	192.168.0.22	00:50:56:90:44:3E				

Document No. 2 of 4   Open with AnalyticConsole

Owner	User/Group	Type	F	M	X	W	R	L	S	Extended Rights
admin@test3.local	[illegible]	Access allowed	F	M	X	W	R	L	S	full access, Traverse / execute file, List directory / file read data, Read attributes, Read attributes extension, Create file / write data, Add subdirectory / file append data, Write attributes, Write attributes extension, Delete, Read permissions, Change Permissions, Write owner
	[illegible]	Access allowed	F	M	X	W	R	L	S	full access, Traverse / execute file, List directory / file read data, Read attributes, Read attributes extension, Create file / write data, Add subdirectory / file append data, Write attributes, Write attributes extension, Delete, Read permissions, Change Permissions, Write owner
	admin@test3.local	Access allowed	F	M	X	W	R	L	S	full access, Traverse / execute file, List directory / file read data, Read attributes, Read attributes extension, Create file / write data, Add subdirectory / file append data, Write attributes, Write attributes extension, Delete, Read permissions, Change Permissions, Write owner
	prof9@test3.local	Access denied	○	F	X	R	R	L	L	Traverse / execute file, List directory / file read data, Read attributes, Read attributes extension, Read permissions
	prof9@test3.local	Access allowed	F	M	X	W	R	L	S	Create file / write data, Add subdirectory / file append data, Write attributes, Write attributes extension

View an incident by security policy

DATA RECOVERY

Case. Before dismissal, the IT specialist decided to take revenge: he uploaded malware to the company's network, which a month later launched the formatting of corporate storage.

Luckily, FileAuditor alerted files deleting from servers. The security manager stopped and deleted the malware, and all affected files were restored from the FileAuditor archives.

How does it work? Shadow copying allows restoring deleted documents or their original versions. FileAuditor enables this function for files that fall under the specified policies. They are automatically encrypted and copied to the storage. To eliminate redundant data, the program implements a deduplication system (a technique for eliminating duplicate copies of repeating data). The deduplication system ensures only one file gets to the storage, not all 50 copies of it. Nevertheless, FileAuditor saves different versions of the same file. Therefore, you can view how the file’s content has been changed in the preview window.

In the scan settings, you can disable shadow copying by selecting the "audit only" mode. In this case, the program will record changes in files, but to view the document itself, a risk manager needs to use a remote PC. Just click on the context menu to do this.

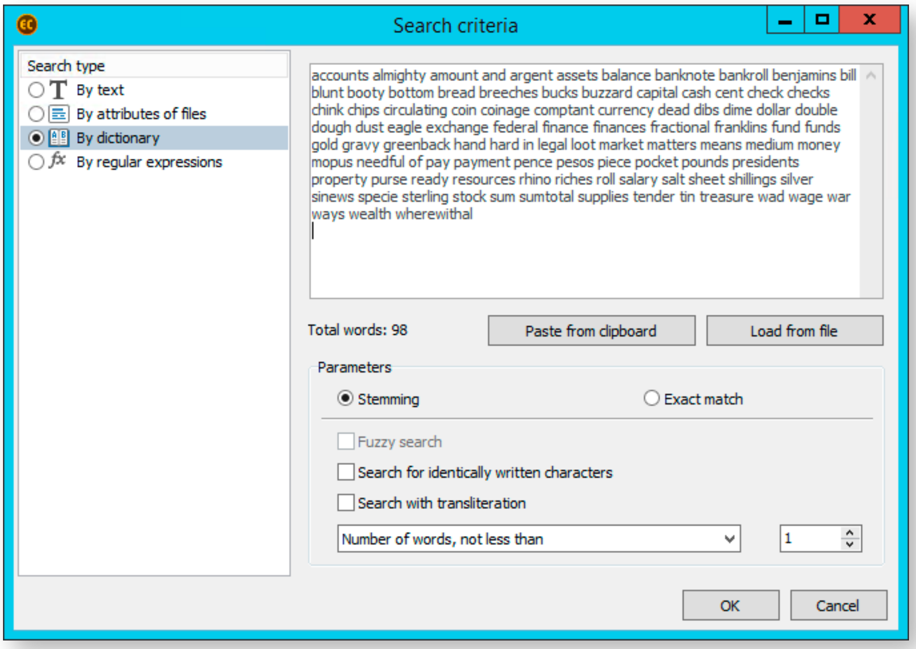
DETECTING FRAUDULENT SCHEMES

Case. The company suspected the purchasing department for taking bribes. FileAuditor detected several employee computers storing Excel documents with internal prices. DLP highlighted that those files were regularly sent to suppliers' external addresses.

After reviewing the documents, it turned out that the tables had a hidden column typed in white font, which contained purchase prices that were several times lower than retail ones.

How does it work? The case demonstrates the benefits of integrating DCAP and DLP solutions. DCAP helps to find clues, and DLP ends the investigation, revealing the bribe-takers by "Price lists" policy scanning.

To prevent such violations, it is convenient to use a dictionary search. For example, the system will identify whether all documents that contain more than 5 words from the financial dictionary belong to the category "Bank statements". You can also include professional and slang vocabulary in the dictionary, which will facilitate bribe-takers discovery.



accounts almighty amount and argent assets balance banknote bankroll benjamins bill blunt booty bottom bread breeches bucks buzzard capital cash cent check checks chink chips circulating coin coinage comptant currency dead dibs dime dollar double dough dust eagle exchange federal finance finances fractional franklins fund funds gold gravy greenback hand hard in legal loot market matters means medium money mopus needful of pay payment pence pesos piece pocket pounds presidents property purse ready resources rhino riches roll salary salt sheet shillings silver sinews specie sterling stock sum sumtotal supplies tender tin treasure wad wage war ways wealth wherewithal

Total words: 98

Parameters

● Stemming ○ Exact match

□ Fuzzy search

□ Search for identically written characters

□ Search with transliteration

Number of words, not less than: 1

Dictionary of financial terms

Have you cleaned your file system? Check it out during the free 30-day trial SerchInform FileAuditor. [I take it!](#)

www.searchinform.com

+44 0 20 3808 4340
order@searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

ABOUT US

SearchInform is the leading developer of risk and compliance software. Our technology secures business against corporate fraud and financial losses, provides for internal risks management, and for human factor control.

Visit our blog to be updated on relevant risk management and data safety issues.

linkedin.com/company/searchinform
facebook.com/SearchInformInternational
twitter.com/SearchinformI