SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INTERNAL THREAT MITIGATION PLATFORM

searchinform.com

1995
The company was founded

Moscow, Russia
head office

2 000 000+
computers are protected by SearchInform software

3 000+ Offices and partners all over the world

6 products enabling comprehensive data protection against threats

2019
SearchInform started to provide monitoring
Services

2020
SearchInform
solution in the cloud
was announced

2018-2020

The Road Show SearchInform
series were held

in **Latin America, the Middle East and North Africa, South Africa, India and Indonesia**

2017

SearchInform software included in
Gartner Magic Quadrant

The Radicati Group
included SearchInform into the **"Enterprise Data Loss Prevention Market, 2017-2021" study**

2010
Training Center
was opened

16 Advanced Training courses for information security professionals

2 Cybersecurity Basics courses for users

PRODUCTS AND SERVICES

SearchInform FileAuditor
Page 4-7

SearchInform DLP
Page 8

SearchInform Risk Monitor
Page 8-18

SearchInform TimeInformer
Page19-20

SearchInform SIEM
Page 21-23

SearchInform Services
Page 24-25

SearchInform integrated solutions
Page 26-27

SearchInform FileAuditor

The amount of data an average company stores is huge. And some of this data contains confidential information: personal and financial data, specifications, drawings, etc. Each group of sensitive data must be stored, processed and distributed in accordance with the corresponding rules.

- IMPORTANT DATA IS ALWAYS IN SIGHT
- FILE PROTECTION IN ANY APPLICATION

SearchInform platform is a COMPLEX MULTILEVEL PROTECTION against information security risks.

LEVELS OF INFORMATION SECURITY insured by SearchInform products:

FIRST LEVEL	SECOND LEVEL	THIRD LEVEL
The file system protection, which is implemented with the help of FileAuditor (DCAP tool).	The DLP system ensures protection at the level of workstations, data channels and human-related risks.	The Risk Monitor implements approach of complex risk and data management protection.

*All the systems are integrated seamlessly, operate on a single technological basis and can be deployed within a few hours. Adding any of the systems significantly increases the functionality of the complex.

IMPORTANT DATA IS ALWAYS VISIBLE

SearchInform FileAuditor is a DCAP solution (data-centric audit and protection) for automated audit of information storages, search for access violations and tracking changes made to critical data. The system protects confidential documents from careless and deliberate malicious actions of employees and puts things in order in file storages.

How FileAuditor solves the problem of monitoring the security of critical data:

Classification of vulnerable data

Finds files in a document flow that contain critical information, and adds a special mark to each file, indicating the type of info it contains: personal data, trade secret, credit card numbers, etc.

Access rights audit

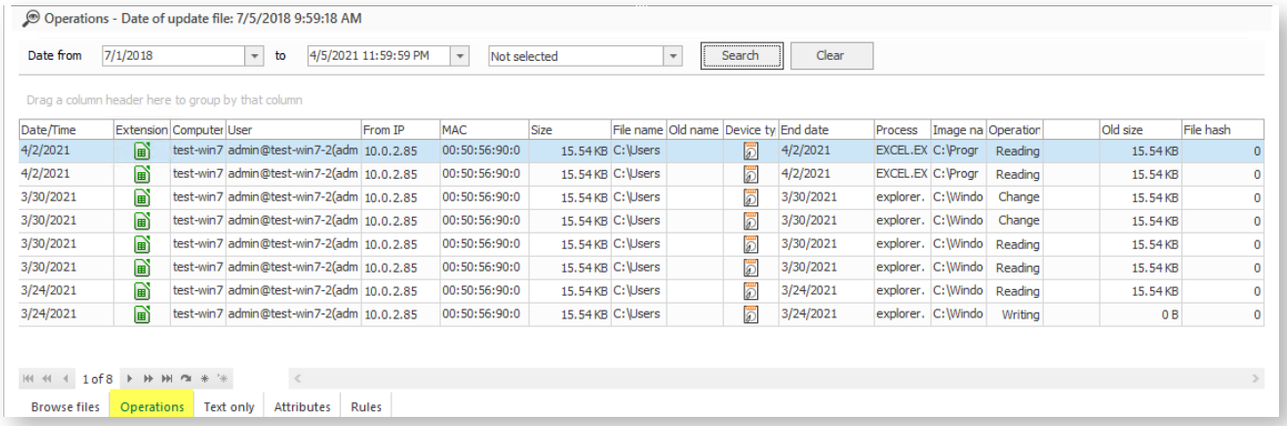
Controls access rights to information (full access, editing, reading, writing, reading and changing, etc.). Tracks employees who have unauthorized access to data. Finds confidential files stored in violation of established security rules (in the public domain, in shared network folders, on employee PCs, etc.)

Critical documents archiving

Makes shadow copies of critical files found on a PC, server or in network folders, saves the history of their revisions. Confidential data archive helps in incident investigation and ensures recovery of lost information.

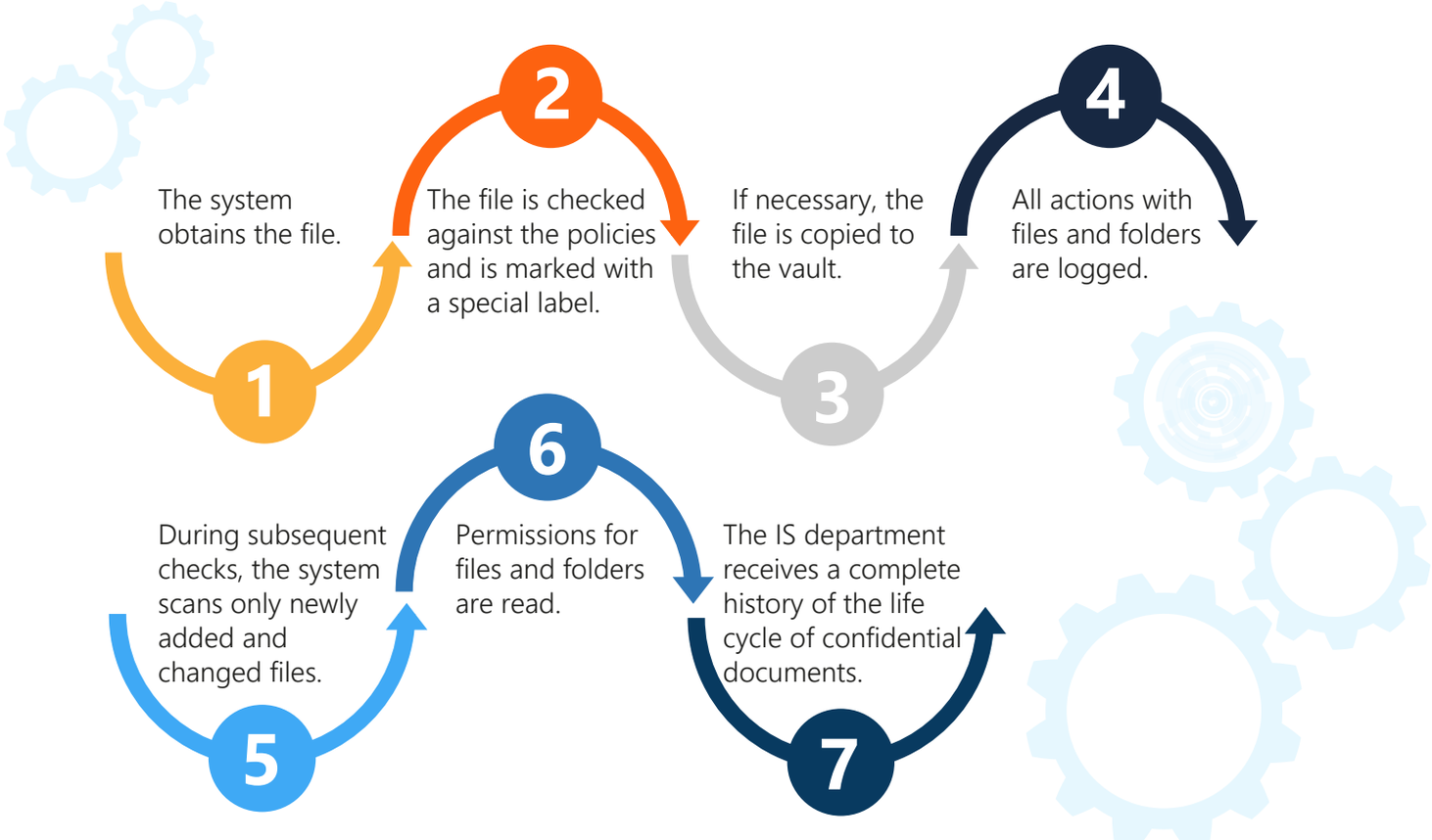
Monitoring and blocking user actions

Audits user operations with the file system. The IT security department is always aware of up-to-date information on the lifecycle of a file (creation, editing, transfer, deletion, etc.). Blocks access to the file and its transfer in any application.



File actions in Active mode

HOW THE SYSTEM WORKS



The collected information is kept in the database, and copies of critical files are maintained. This ensures that documents remain available even after deletion.

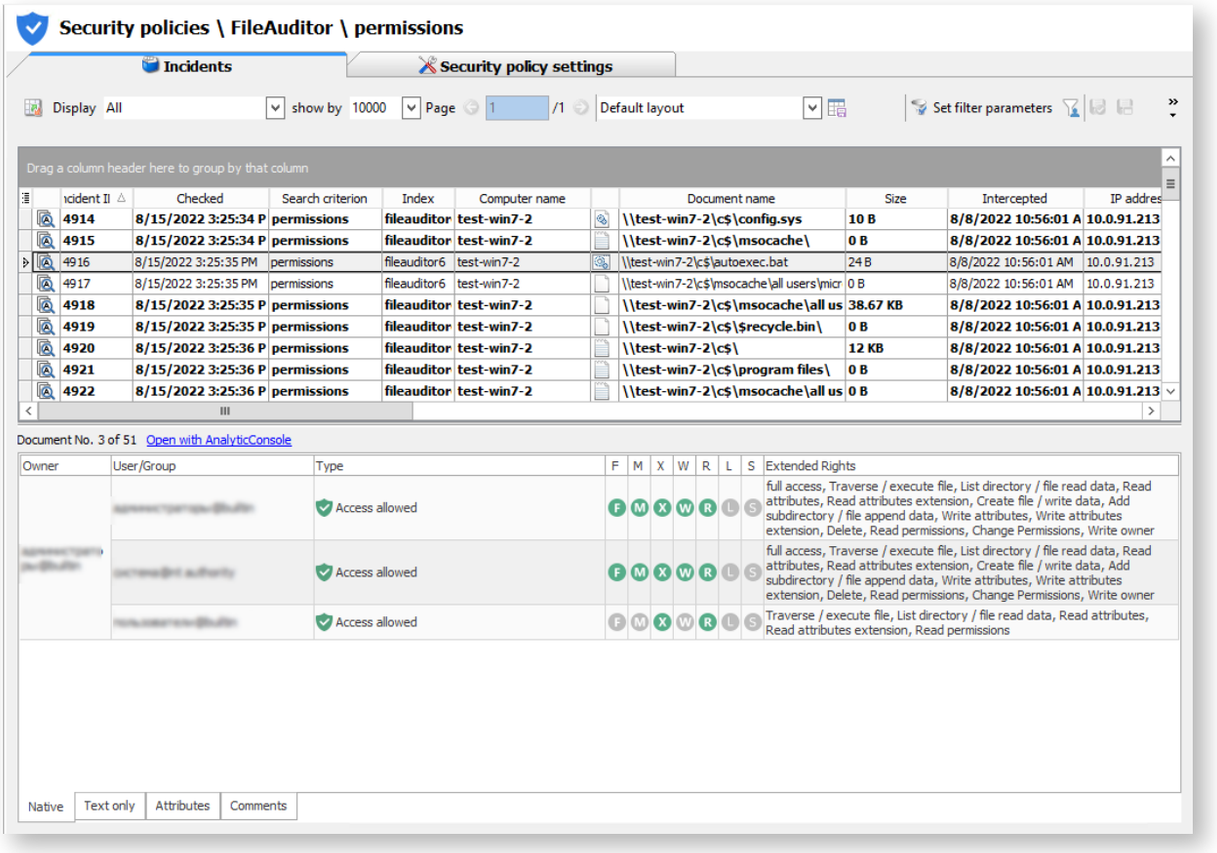
DATA ANALYSIS

FileAuditor analytical module visualizes results of scanning a file system in accordance with rules set. Rule settings have different search types available. Search results can be viewed in the format of visual reports (on sources, access rights, errors) or of a tree.

The program demonstrates:

- Folder tree indicating user rights to each directory or file
- Operations on critical files, creation and modification dates
- Number of critical documents on a disk or in a folder
- File marking (confidential agreement, personal data, financial statements)

Notifications about set policy violations can be configured in AlertCenter. For example, if FileAuditor finds a sensitive document on a PC of a user who has no rights to read it, a specialist responsible for risk mitigation will be alerted automatically as a notification gets emailed shortly.

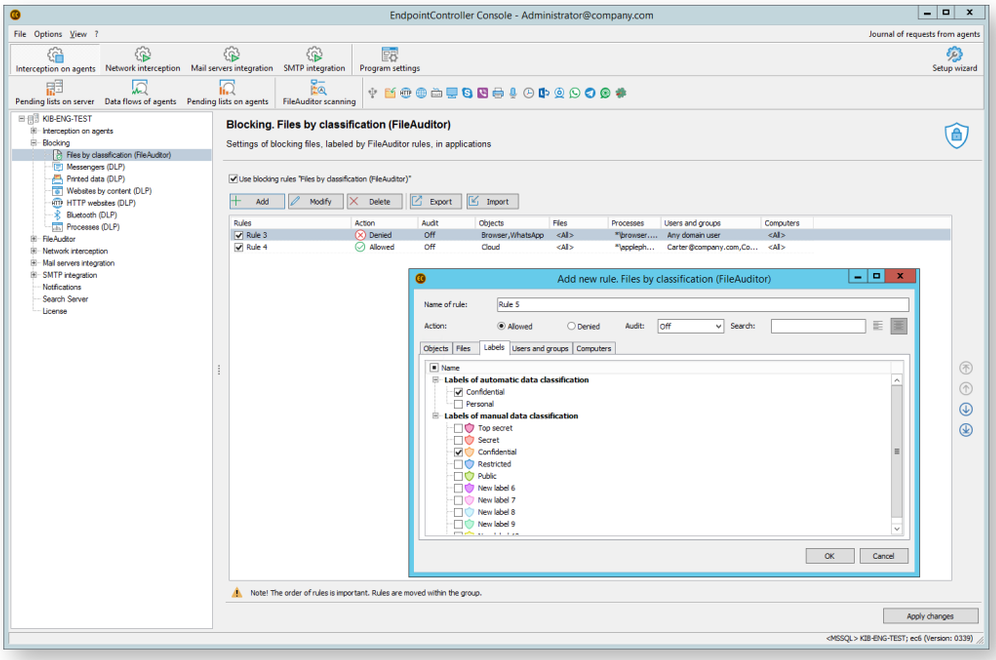


Triggers in the AlertCenter

Information collected by agents and the network scan module is written to a database running Microsoft SQL Server, and copies of critical files are stored within the repository. That is how documents are available even after deletion.

DATA PROTECTION

Restricting file operations: blocking unauthorized operations with documents in various applications, blocking suspicious transfers and access by unauthorised persons. Block commands are applied to automatic and manual classification labels. The system assigns labels to files depending on the category of information - "trade secret", "personal infromation", "contracts", etc. Permissions and blocks are configured in line with information classification and specify to which users, which PCs and which applications it's allowed to interact with the files.



Setting blocking rules by tags in SearchInform FileAuditor

FileAuditor allows blocking access to a file through any application, regardless of the version, type, origin. Restrictions work in the file system, from where it prohibits/allows applications to read data. Thus, you can control the processes of reading, modification, forwarding of documents with confidential data and enable other options for file access.

ADVANTAGES

- Seamless integration of a DCAP-solution into Risk Monitor significantly extends the functionality of the system for risk mitigation
- PC load control and memory saving – monitoring can be scheduled or provoked by a particular event or condition; it's possible to keep only sensitive documents; a deduplication system saves storage space
- Ability to deploy and operate the software in the cloud. The software can be deployed in the cloud, which allows companies that do not have their own IT infrastructure to use the system.
- Due to customizable rule settings specialists don't have to deal with unnecessary tasks and can focus on monitoring only critical data.
- Changes made to files can be tracked almost instantly – the system saves a specified number of file revisions which helps during internal investigation
- Proactive protection of files from changes and transfers. The system can be configured to block access to documents to prevent unwanted user actions with the files.

SearchInform DLP

Protects a company from confidential information leakage, controls data at rest and data in transit.

Monitors all popular data transfer channels, analyzes information, detects and prevents violations, provides reports to a person in charge.

SEARCHINFORM DLP HELPS BUSINESSES IN MANY WAYS

- Protects confidential information from leakage during storage, use and transfer
- Takes control of remote access and virtualization tools (TeamViewer, RAdmin, RDP)
- Facilitates software and hardware inventorying
- Encrypts data to prevent it from being used outside the company
- Reports irregular events within the network, such as copying data to removable storage devices or deleting a large number of files

THE DLP SYSTEM AND FILEAUDITOR INTEGRATION ADVANTAGES

The integration benefits:

Reduction of the DLP system configuring time

Reduction of amount of false positives

Enhance of the organization protection

The DLP system is integrated seamlessly with the FileAuditor. It's easy to configure the DLP system policies according to FileAuditor marks.

SearchInform Risk Monitor

SearchInform provides a comprehensive approach to internal monitoring by extending a DLP solution and blending two powerful concepts: incident prevention and internal threat mitigation.

The instruments for internal threat mitigation and insider risk identification protect your business from financial and reputation losses caused by internal threats.

SEARCHINFORM SOLUTION IN THE CLOUD

Businesses don't have to choose between security, usability and cost because the solution can be deployed in the cloud. No special hardware is required: the system collects, processes and stores data in a virtual environment. Such deployment model will be suitable for companies which don't have their own IT infrastructure, have offices located in different cities, have a big number of employees working remotely.

EXTENDED SOLUTION:

- Detects malicious insider incidents involving corporate fraud and profiteering
- Facilitates regulatory compliance and investigation processes
- Controls the human factor and predicts HR risks
- Operates as an early warning system discovering a potential threat or a precondition for a violation and alerting to possible risks

Risk Monitor provides you with an automated highly perceptive toolset for employee monitoring, risk assessment, and internal auditing, makes sure that corporate policies comply with regulators, and evaluates the conformity of a company's security level to the most recent requirements.

The solution facilitates the creation of the risk management program.

The goal of the proper risk management program is to review operations in order to ascertain that results correspond to the expectations from the established objectives and that operations are being carried out as planned.

Although accidental losses due to human activities are often unanticipated, SearchInform solution can safeguard a company against internal incidents. A risk management framework is at the core of the SearchInform software, helping to make corporate fraud predictable and financial losses preventable.

OBJECTIVES

- Collects detailed information about user activities for step-by-step reconstruction of a violation
- Safeguards a company against personnel risks and predicts employee behavior patterns
- Creates an archive of intercepted information, which facilitates regulatory compliance and security policies enhancement to minimize risks
- Helps to increase staff productivity and assists with team loyalty management
- Alerts to a potential threat before an incident happens, thereby promoting a corporate security culture and boosting internal threat awareness

INFORMATION CAPTURING

SearchInform solution consists of the modules, each of them controls its own data channel.

MailController

Captures all the outbound and inbound mail sent via mail clients and web services, including Gmail, Yahoo, Hotmail, etc. It detects sending messages to private e-mails and e-mail addresses of competitors and blocks the transmission of messages if their content compromises confidential corporate data.

MonitorController

Takes screenshots and records videos of onscreen activity. Supplements the photo and video footage with then-current information about open windows and ongoing processes. If necessary, displays information in real time. Takes snapshots to identify an intruder, recognizes attempts to take a picture of the screen with the help of mobile phone.

IMController

Tracks chats, message history, calls and contact lists in messengers: Skype, WhatsApp, Telegram, Viber, Lync, Gadu-Gadu, XMPP, etc. Monitors correspondence via web services in social media, such as FB, Google+, LinkedIn, etc.

ProgramController*

Collects data on user activity during the day and on time spent in applications, programs and on websites. Automatically determines whether an employee is working or has just launched the program for the appearance of doing something. Categorizes web resources: dating, music, shopping, news, etc.

Helps you monitor remote employee performance

HTTPController

Captures and indexes files and messages sent via HTTP/HTTPS. If necessary, it blocks web traffic, including web messengers, cloud services, mail, blogs, forums, social media and search queries. Maintains its regular surveillance functionality even if employees use anonymizers.

CloudController

Controls files received in, uploaded to, and stored in cloud storages. Tracks cloud storage and file sharing services: Google Docs, Office 365, Evernote, iCloud Drive, SharePoint, Dropbox, Amazon S3, DropMeFiles, etc. Intercepts files sent and received through TeamViewer, RealVNC, Radmin, LiteManager.

FTPController

Checks regular (FTP) and encrypted (FTPS) traffic and notifies the executive of incidents or blocks the connection.

DeviceController

Captures and blocks the data transferred to flash drives, external hard drives, CD/DVD, via RDP and cameras. Automatically encrypts data written to a flash drive. It detects and recognizes smartphones connected to a PC (Android, Apple, BlackBerry, Windows Phone), analyzes their contents when connected in drive mode. It controls device access to a PC.

MicrophoneController

Uses any detected microphone to record talks inside and outside the office. Turns on audio recording – even before the user logs in – when speech is detected or when certain processes and programs, as specified under the relevant security policy, are launched. The audio stream can be converted to text, which is also checked against the specified security policies.

Keylogger

Captures keystrokes and data copied to the clipboard. Intercepts login and password data to facilitate the tracking of accounts maintained on potentially harmful web resources. Identifies users who have entered passwords on their keyboards to access encrypted documents.

PrintController

Inspects the contents of documents sent to print (text files are simply copied, and document scans are intercepted as digital "fingerprints" with their textual content recognized). Detects documents authenticated by a seal and monitors the printout of controlled-issue forms.

CONTROL CENTER

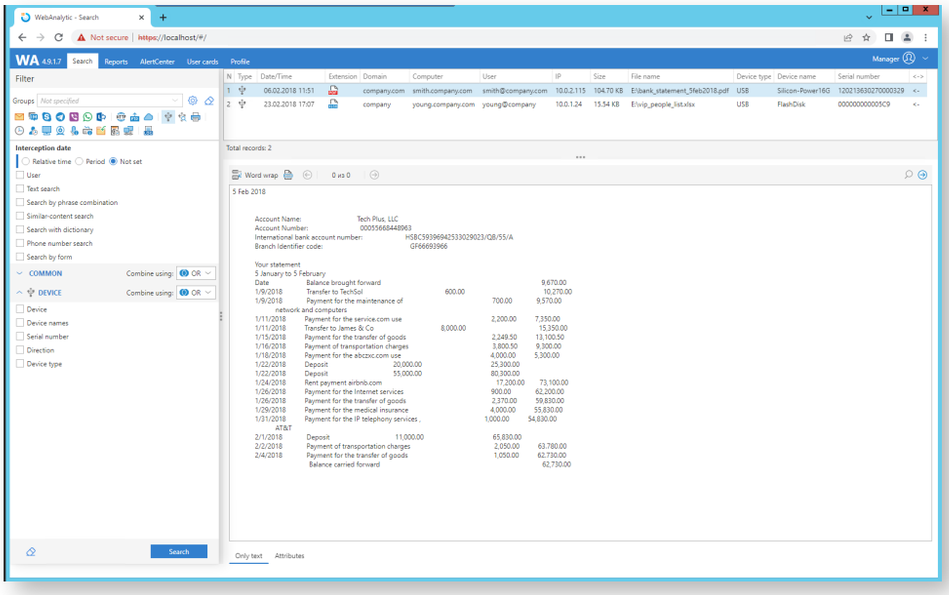
DataCenter

Manages product indexes and databases, monitors system health and ensures connectivity to third-party systems, like AD, SOC, outgoing mail server. DataCenter users can configure the differentiation of access rights.

AlertCenter

This is the system's "think tank" where security policies are set up. It includes 250+ preconfigured security policies that can be edited. The solution makes it possible to create custom rules of captured data scanning and blocking, configure the schedule of checks and send notifications.

You can view incidents in the AlertCenter console on the corporate PC of a responsible person or via the web interface accessible from a laptop, tablet, smartphone.



Search module in SearchInform Risk Monitor web console

Analytic Console

Its objectives are to browse through intercepted data and analyze it as well as to monitor user activities online. Various search algorithms and preset report templates are at the expert's disposal.

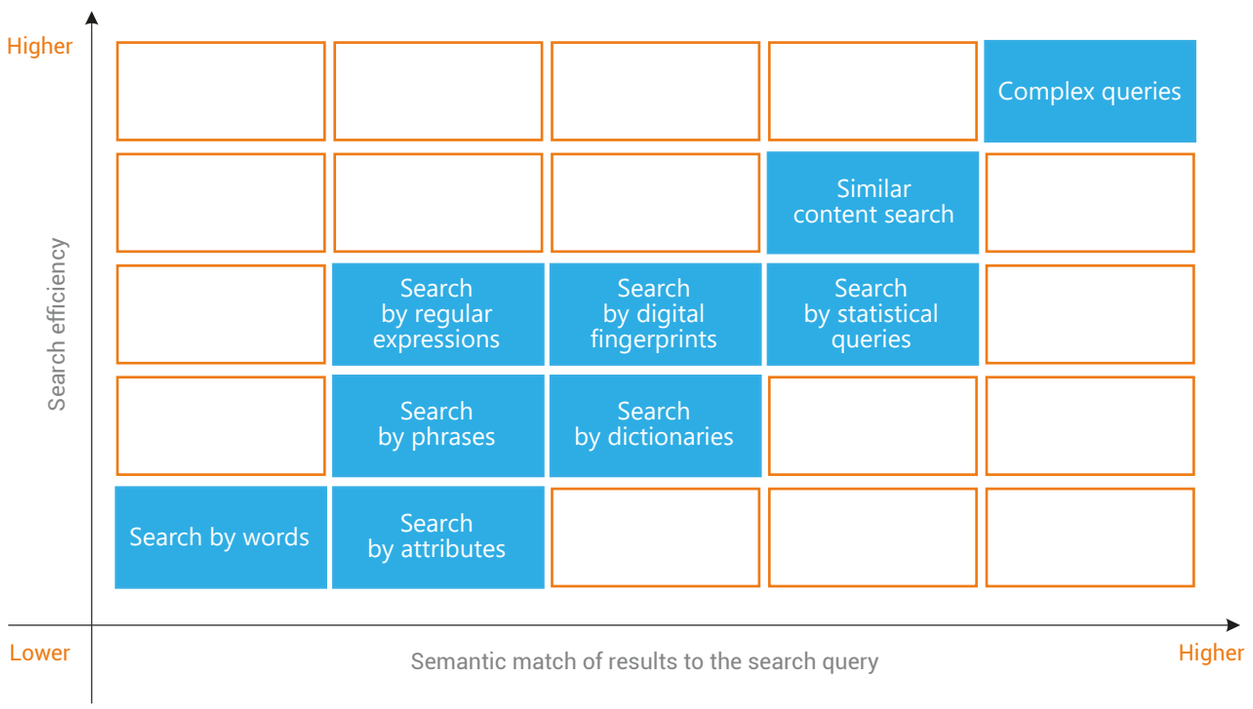
All the functionality of AlertCenter and Analytic Console, including policy creation, viewing incidents and reports, conducting investigations, is now available through the web interface. This makes protection mobile.

ANALYTICAL CAPABILITIES

To perform their functions effectively, experts must have comprehensive control capabilities across all communication channels as well as adequate functionality for searching through captured data and analyzing it. A powerful analytical module, various search options and automated graphics and audio analysis allow just one specialist to inspect the work of several thousand employees.

Text analysis

A variety of algorithms provides in-depth verification of text messages and documents, for instance, there are unique search technologies such as Similar Content Search or Complex Queries. The proprietary Similar Content Search algorithm identifies confidential documents even if they have been edited, which means that the search results will include documents that match the query semantically rather than just technically. Complex queries allow the user to construct an advanced search algorithms using simple queries logically combined by AND, OR and NOT operators.



Graphics analysis

The system determines the types of images circulating within the company: PDF-files, photos or scanned copies – and categorizes image files accordingly. The integrated OCR (Optical Character Recognition) system identifies documents that conform to specified patterns: passports, bankcards, driving licenses, etc. The technology allows finding personal, financial and any other sensitive data in the archive, even transmitted in the format of scanned documents.

Audio analysis

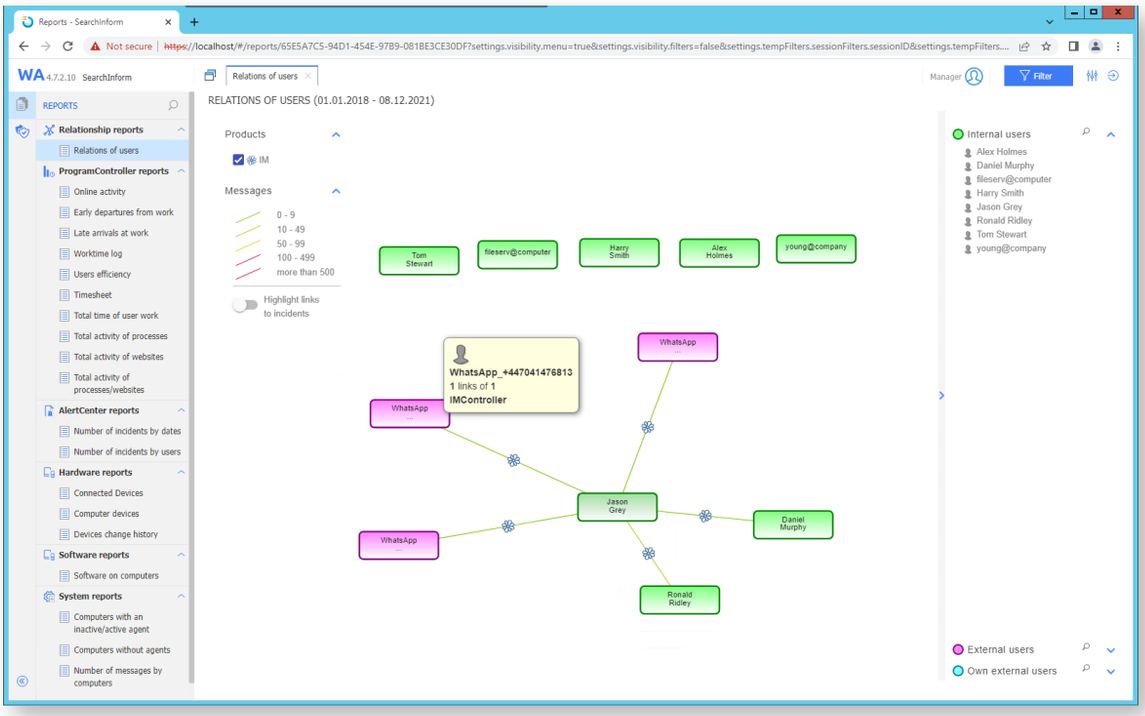
SearchInform solution converts audio records into text and checks whether a transcript complies with the security policies. The system has an option to turn on audio recording when speech is detected or when certain processes or programs, as specified under the relevant security policy, are launched.

REPORTS & UEBA

SearchInform software visualizes all the events and connections within the company in the form of reports – via Analytic Console and web interface. The default configuration includes more than 30 basic templates. The report wizard allows the user to create custom reports not limited by any criteria.

RelationsChart report

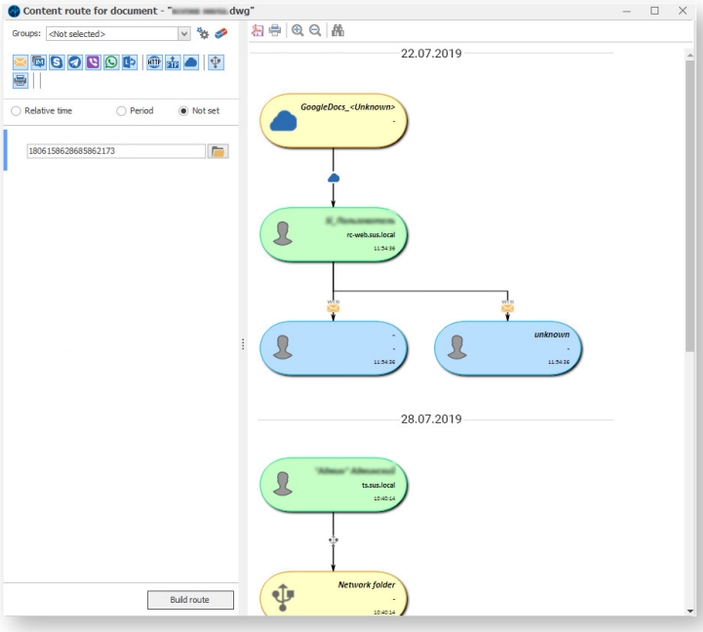
Demonstrates employee-to-employee and employee-to-third-party connections in the form of a relational graph. Visualizes user activities across all communication channels or within a particular communication line. Facilitates corporate investigations.



Analytic Console relational graph

Content routing report

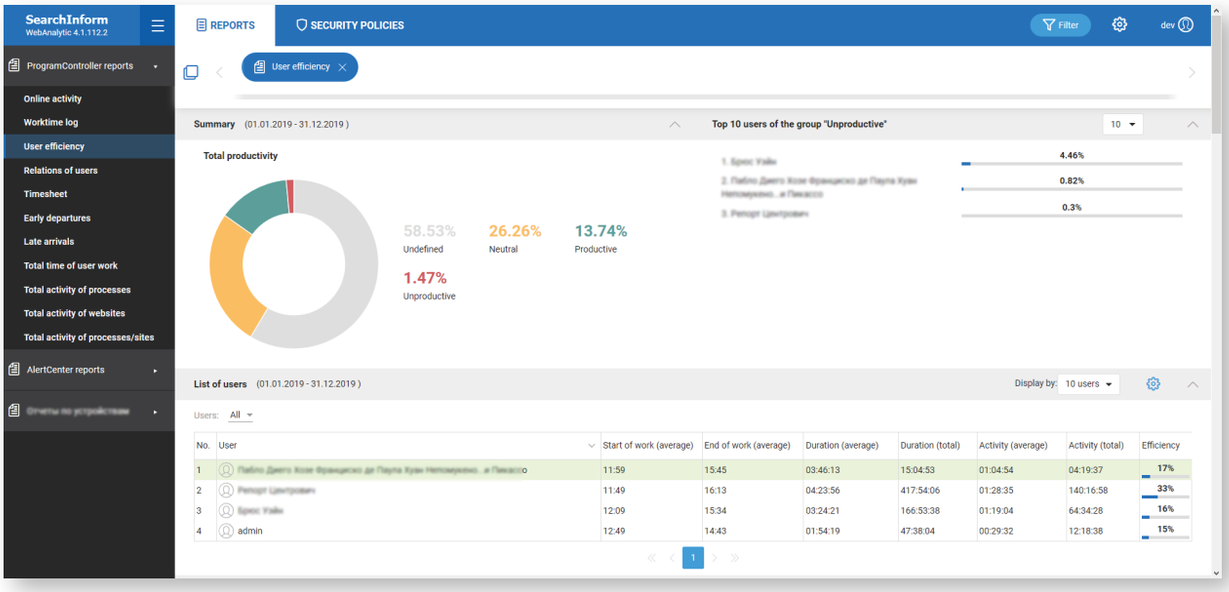
Makes all the document movements between the sender and the recipient via internal and external communication channels completely transparent. Enables prompt identification of the document's author as well as the source of the respective information and the paths of its distribution.



Content routing

User productivity report

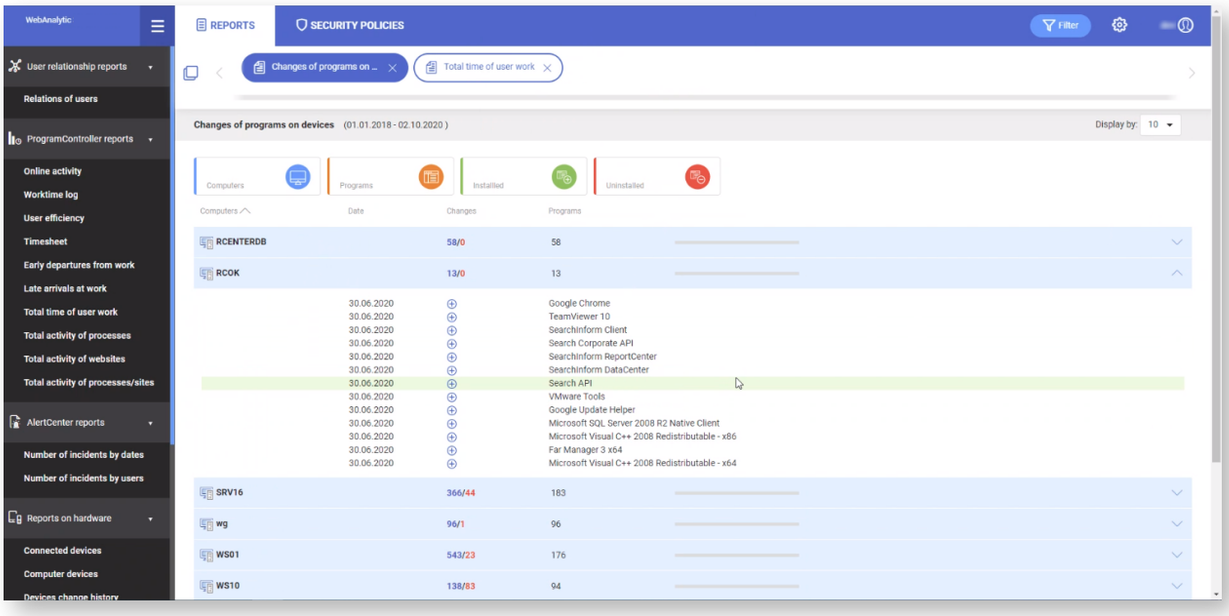
Shows the overall productivity of company employees in charts and ratings. It detects how often employees get early at/off work, and those who are frequently late at work. Visualizes user performance during the workweek in a calendar format.



User productivity report

Software and hardware report

Reports any changes to installed hardware and connected devices. This facilitates inventorying and safeguards against equipment theft or unauthorized equipment substitutions. Software reports structure data on software installation and uninstallation operations.

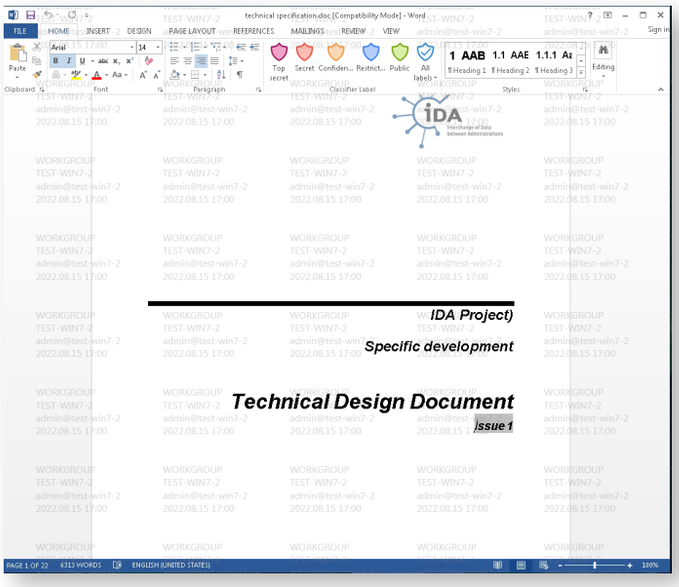


Software and hardware report

INVESTIGATIONS AND CONTROL

Leak detection when leaks are conducted through taking screenshots and screen photos

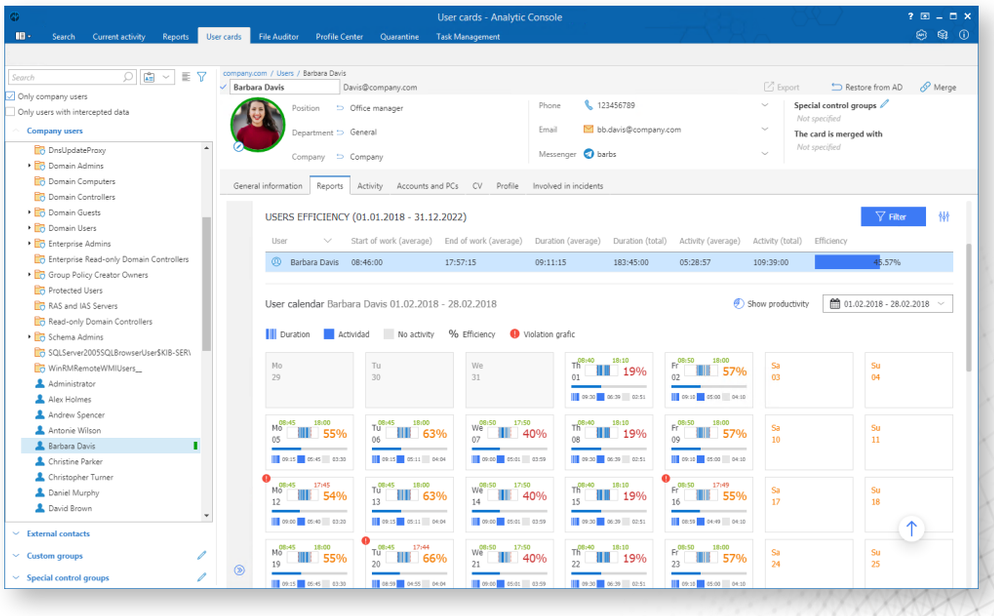
Detecting the source of the leak, when a user is taking screenshots or screen photos is extremely hard. Thanks to Searchinform Risk Monitor and its watermarking tool this is becoming increasingly easy. When a screenshot or a photo is taken on a protected computer, a search in external sources allows information security specialist to determine easily the source of the leak. The watermark contains an indication of the PC and the employee who works on it.



Watermarks created by Searchinform Risk Monitor

User card

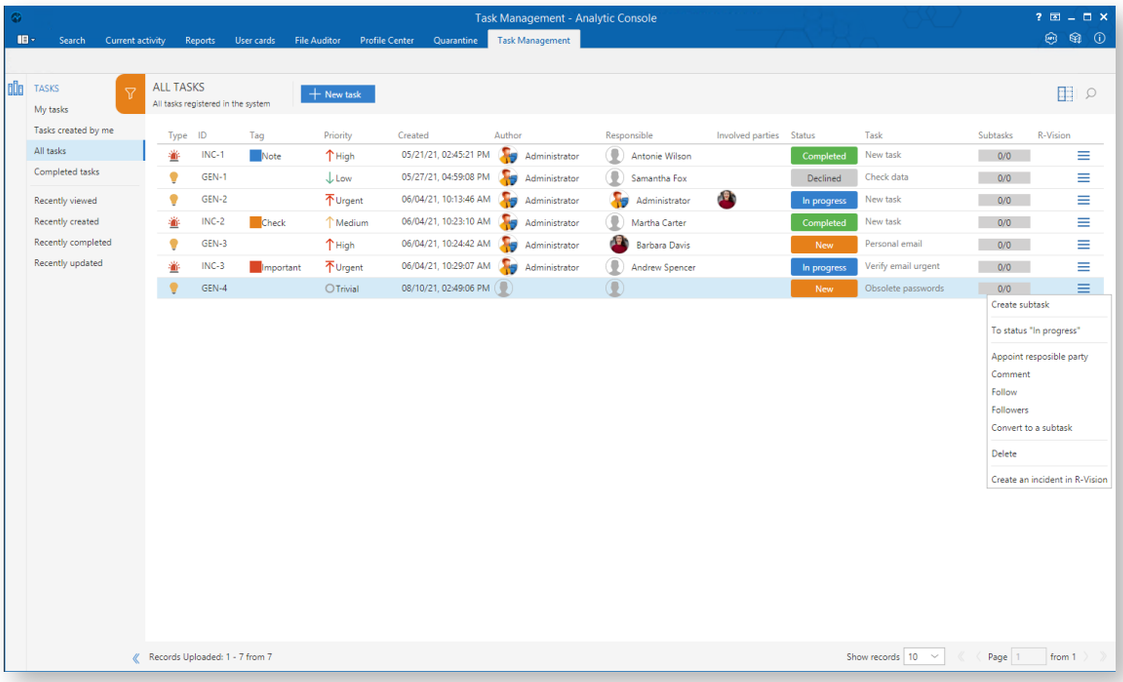
User card collects a "dossier" on each employee, automatically including all the incidents in which he/she participated. User card contains individual reports, biographical and contact details of the employee, his/her job history.



User card

Investigation Management

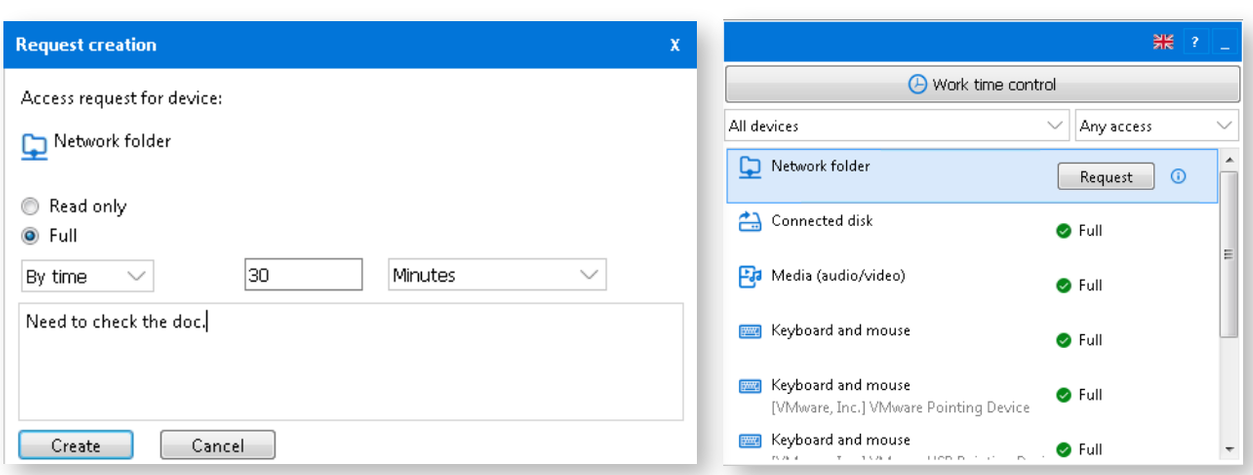
Task Manager enables coordination of information security tasks conducted by IT security specialists. Task Manager also allows distribution of tasks, tracking the progress of investigations and generating reports on the results of such investigations - including their transfer to the SOC.



Task Management tool

User interface

Notifies employees about working time controls, active permissions or access denials. User interface allows sending direct requests from the information security service to use flash drives and other devices. The information security specialist can issue permits for the requested period, change the access period or revoke the permission during the session if an incident is suspected.



User interface

The "open" control mode using the interface on user PCs improves the discipline of employees and reduces the load on the information security department.

UNIQUE FEATURES

1 Unique analytical features unavailable in any other tool

Apart from conventional analytical features, such as search using dictionary, regular expressions, digital fingerprints and OCR, SearchInform Risk Monitor can boast such features as search for images similar to the original, search in any audio recordings (using speech-to-text technology), and content search in video recordings of user's activity to check only activity of interest.

2 High quality investigation tools in one solution

The solution enables recording audio of user's speech and video of user's actions, logging all kinds of user's operations with files and folders, audit logs, devices and software, as well as monitoring violators via audio and video channels in real-time.

3 Control of user's work efficiency

SearchInform Risk Monitor automatically evaluates user's work efficiency in various applications and on web sites. This function helps to strengthen discipline in a company and detect existing problems with business processes.

4 Confirmed system stability under load

Among SearchInform's clients, there are large-scale enterprises from various business spheres. This fact illustrates that the system operates stable in different IT environments and under high load.

5 Extension of features by using products of the same vendor

SearchInform offers a range of products, which includes Risk Monitor, DLP, SIEM and FileAuditor (DCAP solution). All the systems operate on the same technological base. They are integrated seamlessly and deployed within a few hours.

6 Cross-platform and accessible from any device

User interface of SearchInform Risk Monitor may be presented in two ways – as the Windows client and as a web version.

ADVANTAGES

Documents content route

It demonstrates the movement of documents, indicates the sender and the recipient, as well as the communication channels used for data transfer.

Cloud deployment model

All the components of Risk Monitor can be deployed in the cloud (SearchInform cloud or any third-party cloud service can be used) not interfering with the system's functionality. This way of data protection is cost-effective and time-saving.

Remote access control

SearchInform solution protects data transmitted through virtual environments and remote control tools. Monitoring is implemented both at the clipboard level, virtual storage devices connection, and at the level of specific software features (for example, transfer via the TeamViewer context menu).

Implementation department and Training Center

Our hands-on experience with 3 000+ companies in different industries allows us to promptly create unique sets of security policies focused on relevant tasks and the customer's specific line of business.

Easy deployment with no changes to the network structure

The customer's own IT specialists will be able to install SearchInform solution within a few hours. The installation process does not hamper the operation of the company's local information systems.

Data at rest monitoring

The system will serve timely alerts upon registering the presence of confidential information in locations not designed for its storage.

Integration with other SearchInform products

SearchInform solution is seamlessly integrated with SIEM, ProfileCenter, FileAuditor, which increases the level of information security and risk awareness of the company, reduces the response time to the incident, makes it possible to fully investigate violations.

Incident Investigation Tools

Online activity control tools, such as recording conversations and capturing onscreen content in real time, monitoring keyboard inputs and making video with a webcam, information flows, connections graphs and user cards, task management for the information security department, automated search for incidents - will help to reconstruct security violations step by step.

Elements of artificial intelligence

The system automatically recognizes the faces of users and helps find whether the PC is not operated by its owner. Risk Monitor captures attempts to take a picture of a computer screen with a smartphone and protects photos of the monitor with unique watermarks to identify the source of the leak.

Proactive Incident Protection

Risk Monitor allows smart content blocking for all controlled channels to ensure users will not be able to transfer files and messages with confidential content. The interface of the agent will warn the user about accidental violation of the policy to promote information security culture.

A powerful analytical module

Offers fast and flexible solutions for configuring alerts and analyzing data streams without hiring third-party specialists. With the help of SearchInform product one specialist can control the work of several thousand employees.

SearchInform TimeInformer

For some employees being at work does not automatically mean dealing with their direct responsibilities. There are always some irresponsible people who take frequent smoke and coffee breaks, chit-chat with colleagues, spend time on social networks, arrive to work late or leave early.

TEAM ACTIVITY

TimeInformer is an employee monitoring solution that protects business from inefficient work and financial losses related to personnel.

TimeInformer will scan work computers and help you identify:

- Violators of working discipline who arrive late, leave early, take frequent smoke and coffee breaks
- Freelancers who do side-work in the hours paid by the company
- Idlers, who chat, shop online, distract to games and other activities
- Unsatisfied employees who turn other workers against employer, or who have got exhausted because of heavy workload or boring tasks

The software determines idleness time and work time of employees, collects data on software employees use during a day, records all visited websites and categorizes them – dating sites, online shopping, news, TV shows, etc. and evaluates the real productivity of the staff according to the given parameters.

CONTROL IN REAL TIME

TimeInformer can be used not only in the background, but in other modes too. The program connects to PC monitors and microphones and reproduces in real time what is happening.

The solution plays or records in real-time mode important negotiations with key partners and clients. TimeInformer shows in real-time mode what is displayed on your employees' monitors at any given time, up to 16 PCs simultaneously.

TimeInformer can be deployed in the cloud providing you the solution with no need to purchase and maintain hardware.

ASSISTANCE IN MANAGEMENT DECISIONS

33 pre-set reports in TimeInformer provide for a smooth start, allow quick detection of idlers, help to optimize work processes, get people organized and goals achieved.

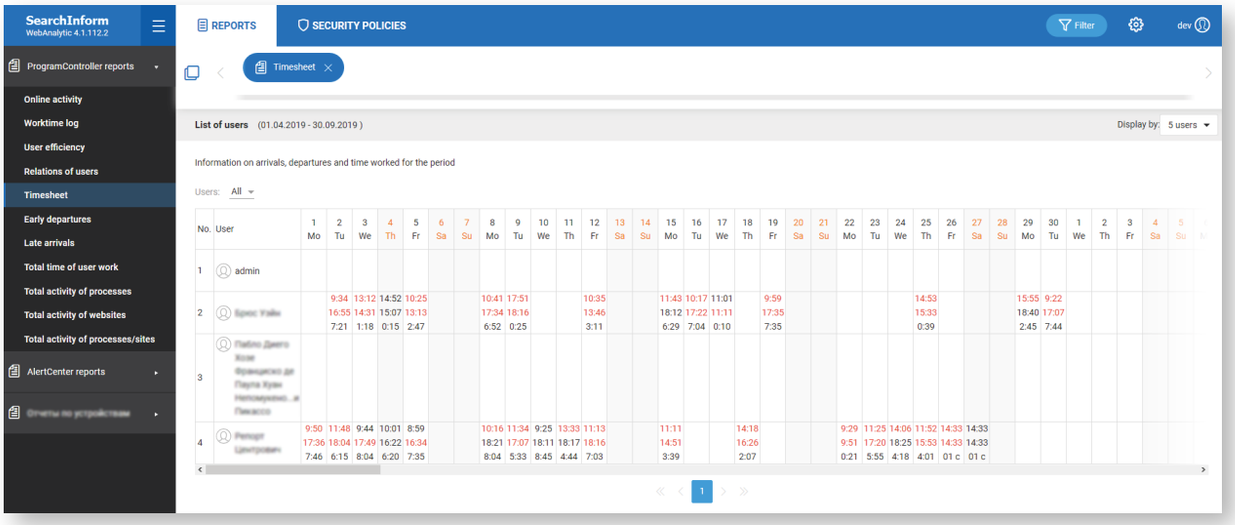
TimeInformer has the following groups of reports:

- Reports on user activity in applications and on websites
- Reports on programs with the history of software installing and deleting
- Reports on devices with data on equipment installed on a PC and changes in their configuration

Reports and notifications are easily customized. The system will send an automatic notification about violation.

USER-FRIENDLY

Web interface will allow controlling employees from anywhere in the world. Permissions to view reports and administration options are differentiated according to tasks and work duties. Automatic alerts about suspicious activity of employees can be received by e-mail.



Timesheet in web interface

ADVANTAGES

- Secure from being deleted and alerts about such attempts
- Monitoring of users' activity even when they work from home or are on business trips
- Web interface to access the monitoring results outside the office
- Integration with SearchInform products, which helps to perform internal investigations

SearchInform SIEM

- FIRST OUT-OF-THE-BOX SIEM
- CREATING CORRELATION RULES IN 2 CLICKS

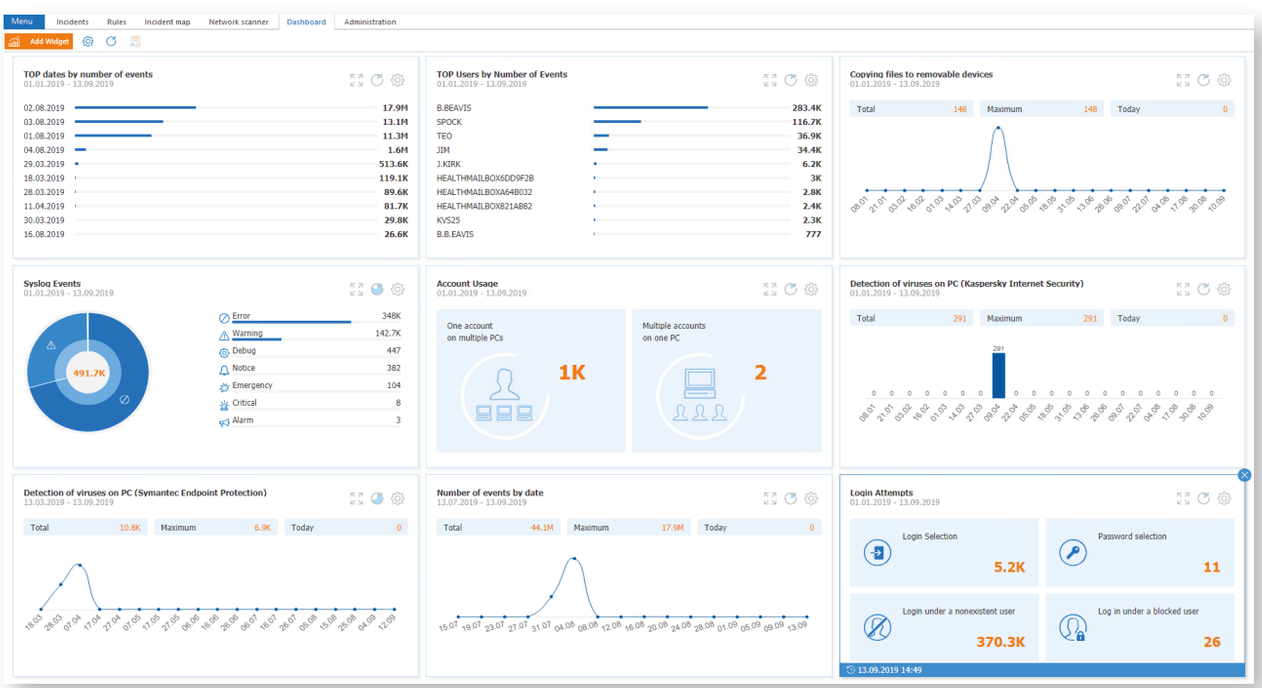
No.1

IT infrastructure of a company includes a multitude of corporate systems: Firewalls, operating systems, email servers, databases, network devices.

Many of these systems are data sources that attract violators, which implies the necessety of special protection.

Automatic security event monitoring

SearchInform SIEM is a system for collecting and analyzing real-time security events, identifying information security incidents and responding to them. The system accumulates information from various sources, analyzes it, records incidents and alerts the designated staff.



Event statistics dashboard

SearchInform SIEM reveals:

- Virus epidemics and separate infections
- Attempts to gain unauthorized access to data
- Account password guessing
- Active accounts of dismissed employees that had to be deleted
- Hardware configuration errors
- Permissible operating temperature abuse
- Data removal from critical resources
- Use of corporate resources during off-duty time
- Virtual machines and snapshots removal
- Connecting new equipment to IT infrastructure
- Group policy changes
- TeamViewer usage, remote access to corporate resources
- Critical events in protection systems
- Errors and failures in information systems

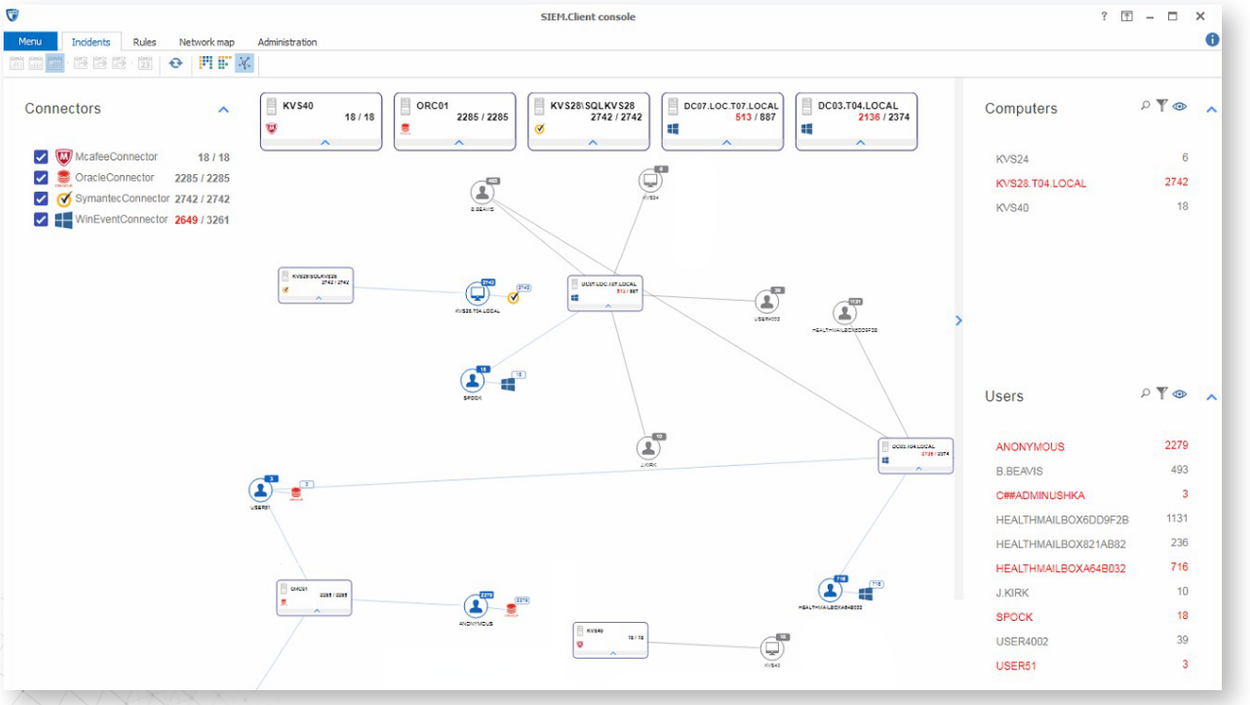
PREDEFINED CORRELATION RULES

Upon the system installation, the information security staff gain access to 300+ ready-made rules – security policies. Users can edit and customize existing rules and create their own policies, i.e. choose from the preset list and add their own policies (user connector function).

Out of the box correlation rules utilise the following data sources:

- Operating systems
- Email servers
- Domain and workstation controllers
- Linux servers and workstations
- DBMS
- DLP systems
- File servers
- Virtualization environments
- Antiviruses
- Firewalls and integrated network security devices
- Solutions on the 1C platform
- Other syslog sources

Cross correlation rules can be configured to search for incidents related to events collected from various sources.



Incident display screen

Ready-made correlation rules in SearchInform SIEM:

For mail servers

- Unsolicited access to the mailbox
- Change in mailbox ownship
- Granting access to the mailbox

For virtualization environment

- Login/logout events for VWview/VMware
- Incorrect passwords
- Removing snapshots

For domain controller and workstations

- Temporary enabling/adding of an account
- One account on multiple PCs
- Password guessing and outdated passwords

To access to file resources

- Access to critical resources
- Temporary issue of rights to a file/folder
- Large number of users working with the file

HOW THE SYSTEM WORKS

1 Collects events from various software and hardware sources: network equipment, third-party software, security tools, OS.

2 Analyses events and generates incidents in accordance with the rules, detects threats by identifying relationships (correlations, including cross-correlations) of events and/or incidents.

3 Automatically notifies employees in charge when incidents occur.

4 Normalises and details incidents for further investigation: determines the type and source of the incident, when integrated with AD – identifies the user.

ADVANTAGES

- Quick implementation without a need for a lengthy pre-configuration (software can be put into operation in just one day with instant results).
- Easy to use: the program can be handled by an employee with no particular IT skills or knowledge of programming languages – none are required to create correlation and cross-correlation rules.
- Low hardware requirements, transparent licensing, comfortable cost of ownership.
- Out-of-the-box analytics: the system comes with a set of ready-made rules and incorporates the previous experience of working with companies from all sectors of the economy.
- Incident management. It's possible to create an investigation based on one or more incidents.

Seamless integration with Risk Monitor strengthens company's information security and makes it possible to carry out a comprehensive investigation of an incident and collect required evidence.

Services

SearchInform provides services to companies which don't have a dedicated risk mitigation department or lack sources to integrate a data protection system and implement monitoring.

Our services allow a company to benefit from the solution which requires minimum financial and labor costs of a client as well as no need to hire specialists. A customer gets the system together with a team of analysts who have vast experience in the field. Experts begin to work straight after deployment without being taken onboard – no training, no vacation, no sick leave.

As-a-service option is available for every SearchInform product. All of them can be deployed in the cloud saving a company's finances as there is no need to buy hardware and spend on its maintenance.

Product	As-a-service	Cloud deployment model
SearchInform DLP	+	+
SearchInform Risk Monitor	+	+
SearchInform FileAuditor	+	+
SearchInform SIEM	+	+
SearchInform TimeInformer	+	+

HOW DOES IT WORK?

A specialist configures the system in accordance with the tasks set by a customer.

A customer gets fully authorized to work with the system.

After an incident is detected, a specialist contacts a customer (means of communication are selected in advance).

A specialist provides a customer with incidents reports which cover a specified period of time (once a day/week/month).

A customer can work with the system together with a specialist or independently.

A customer can assign tasks to a specialist.

TASK – SOLUTION

Our services allow to detect weak spots in a company in a short period of time (first results are obtained within 1-3 months).

The specialists who work with the customer monitor the solution deployment, and also perform decision-making based on the results of reports and incident investigation.

Summary report on the incidents. Details on each incident are availble in the folder with the incident number.					
No.	**Date**	**Employees related to the incident**	**Incident overview**	**Comment**	**Link to documents**
			Confidential data		
1		Employee name	Copied some databases with name 'BASE C1' to USB drive.	It is not clear why the employee copied some strange	Link+RCI-
2		Employee name	Copied files in .cnc format to USB drive. The files appear to be some programs for machine tools.	The question is why.	Link
3		Employee name	Copied corporate documents to flash drive.	Not clear why the employee did it.	Link
4		Employee name	Copied a file with the name 'Efficiency' to USB drive.	Not clear why the employee did it.	Link
5		Employee name	Numerous corporate documents were copied to USB drive.	Not clear why the employee did it.	Link
			Job search		
6		Employee name	Chatted with a friend on Facebook on her plan to leave the current job in her native town and find a job in Moscow.	Job search.	Link
7		Employee name	The employee's receiving e-mails from hh.com with recommended vacancies and CV views.	Job search.	Link
8		Employee name	On Facebook sent a CV of her husband, emloyee of the same company, to her daughter.	Probably, to be sent to a would-be employer.	Link
			Forgery of documents		
9		Employee name	Forgery of documents in Paint.	Set a client's stamp and signature on the specification.	Link
10		Employee name	Edition of the corporate stamp in Photoshop.	Not clear why the employee did it.	Link
11		Employee name	Forgery of documents in Paint.	Stamped the specification document.	Link
			Side companies		
12		Employee name	Downloaded from GoogleDocs various invoices, payment documents in which there were specified different company names. All of them were headed by Employee 12.	Side company.	Link
			Discussion of the management		
13		Employee name	In Paint, was drawing on the director's photo.	Mocking the management.	Link
14		Employee name	Discussion of the management on Facebook.	Discussion of the management.	Link
15		Employee name	In the correpsosnde on WhatsApp, was discussing the director mentioning one manager.	Discussion of the management.	Link
			Big-budget purchases		
16		Employee name	The employee had correspondence with a project developer about participation interest in buying a flat.	Discussed flat payment terms.	Link
17		Employee name	Printed out an apartment equity construction agreeemnt.	The agreement included sums of money of own participation and credit amounts.	Link
			Entrepreneurship and side jobs		
18		Employee name	Documents sent to a cloud storage made it clear that the employee was a independent entrepreneur and provided services, including to the company he worked in.	Likely to have side job damaging the current company.	Link
19		Employee name	Received e-mails to personal e-mail account with offers of odd jobs	Possible side job.	Link
20		Employee name	The employee sent and downloaded documents to/from iCloud, which made it clear he had own business.	The employee provides legal services to different companies gaining significantly.	Link
			Ambiguous relationship		
21		Employee name	The employee sent several CVs from personal e-mail accountto to another employee.	Possibly wants to find employment for family.	Link
22		Employee name	Chatting on social network telling about some aquaintance drug addict from Poland who has weapon. Also, telling about her being sexually abused.	Suspicious relations.	Link
23		Employee name	Correspondence on Facebook about intimacy intention meetings.	Suspicious relations.	Link
			Disappointed customers		
24		Employee name	E-mail from a disappointed dissatisfied client in which he complains on the work.	Disappointed client.	Link
			Entrepreneurship and side jobs		
25		Employee name	Too close communication with one client.	Friendly communication with one client who asks to give good prices. Payoffs are possible.	Link
			Miscellaneous		
26		Employee name	Reading reviews on work in the company.		Link
27		Employee name	Watching movies in work time, some days for more than 5 hours.	Misuse of work time and resources.	Link
28		Employee name	In Viber chat wrote that there was a new manager in the company and not clear what to expect.	Discussion of the management.	Link

Brief report on incidents

ADVANTAGES

- An unbiased attitude and professional approach – the team of analysts providing our services don't know the employees in person, therefore, the human factor during the investigation is excluded.
- Sharing the experience and knowledge of the company with 3 000+ clients. Our team will be able to fine-tune the software taking into account the scope of a company, as well as to help an organization procure maximum benefit from the system functionality.
- Detection of "pain points" of the company in a short period of time (the first results are usually obtained within 1 month).
- Low entry threshold: no need to spend money on equipment and salary of information security specialists, and time to implement the system. All this is included in the monthly subscription for information security outsourcing.

SearchInform integrated solutions

SEARCHINFORM AND HUAWEI

SearchInform FileAuditor and Huawei OceanStor joint solution provide an organisation with a seamless integration allowing you to use all the file auditing functions, including categorisation, checking of access permissions, audit of operations with confidential information, on OceanStor SAN devices.

Large data storage systems capable of managing massive data arrays and allowing access for multiple users are unavoidable nowadays. The issue is that such storages require impeccable compliance with security rules and ensuring a high level of data protection.

In order to store data safely and be aware of where confidential information is located, who uses it or makes any changes, it is important to equip corporate systems with smart analytics and accompany the storage with a file auditing tool.

- Classification of vulnerable data
- Critical documents archiving
- Access rights audit
- User activity monitoring

- A company gets a single solution as SearchInform FileAuditor and Huawei OceanStor are smoothly integrated
- No need to deploy third-party solutions and make them work together
- Built-in options of audit of operations with information and access control list
- Automated categorisation of stored data based on its content
- Permanent isolated storage of shadow copies of sensitive files
- Detection of storage violations and access misuse

SEARCHINFORM AND MICROSOFT

SearchInform offers a fully-functional system now available in Microsoft Azure – the reliable cloud solution ensuring conformity to standards and requirements set by multinational companies and government organisations.

Microsoft Azure

Microsoft Azure is supported by 3500 cybersecurity experts providing customers with highly protected infrastructure and working process. Azure takes care of an enterprise's data as an organisation controls its corporate data completely, sharing for marketing purpose is forbidden. The marketplace lets vendors present versions of their software adapted for work in virtual environment.

Cooperation with Microsoft makes SearchInform instruments for data protection and internal threat prevention available anywhere in the world, as being presented on the platform guarantees quality and applicability within Microsoft norms and rules.

Follow these 4 steps to deploy SearchInform solution in Microsoft Azure:

1. Choose our product in Azure
2. Opt for a data storage system and DBMS location
3. Submit for licenses and install them in the Data Center
4. Deploy the software on PCs

CONTACTS

ARGENTINA
Buenos Aires
Phone: +54 0 11 5984 2618
+54 9 11 5158 8557
Email: r.martinez@searchinform.com

BELARUS
Minsk
Phone: +375 17 227 56 80
Email: order@searchinform.ru

BRAZIL
Sao Paulo
Phone: +55 11 9 8973 2037
Email: s.bertoni@searchinform.com

KAZAKHSTAN
Almaty
Phone: +7 705 188 98 85
+7 777 239 30 36
Email: d.stelchenko@searchinform.ru

MENA
Phone: +375 33 344 85 90
Email: yamen@searchinform.com

RUSSIA
Moscow (head office)
Phone: +7 495 721 84 06
+7 499 703 04 57
Email: info@searchinform.ru

SOUTH AFRICA
Centurion
Phone: +27 12 683 8816
Email: jorina@searchinform.com

OUR CLIENTS