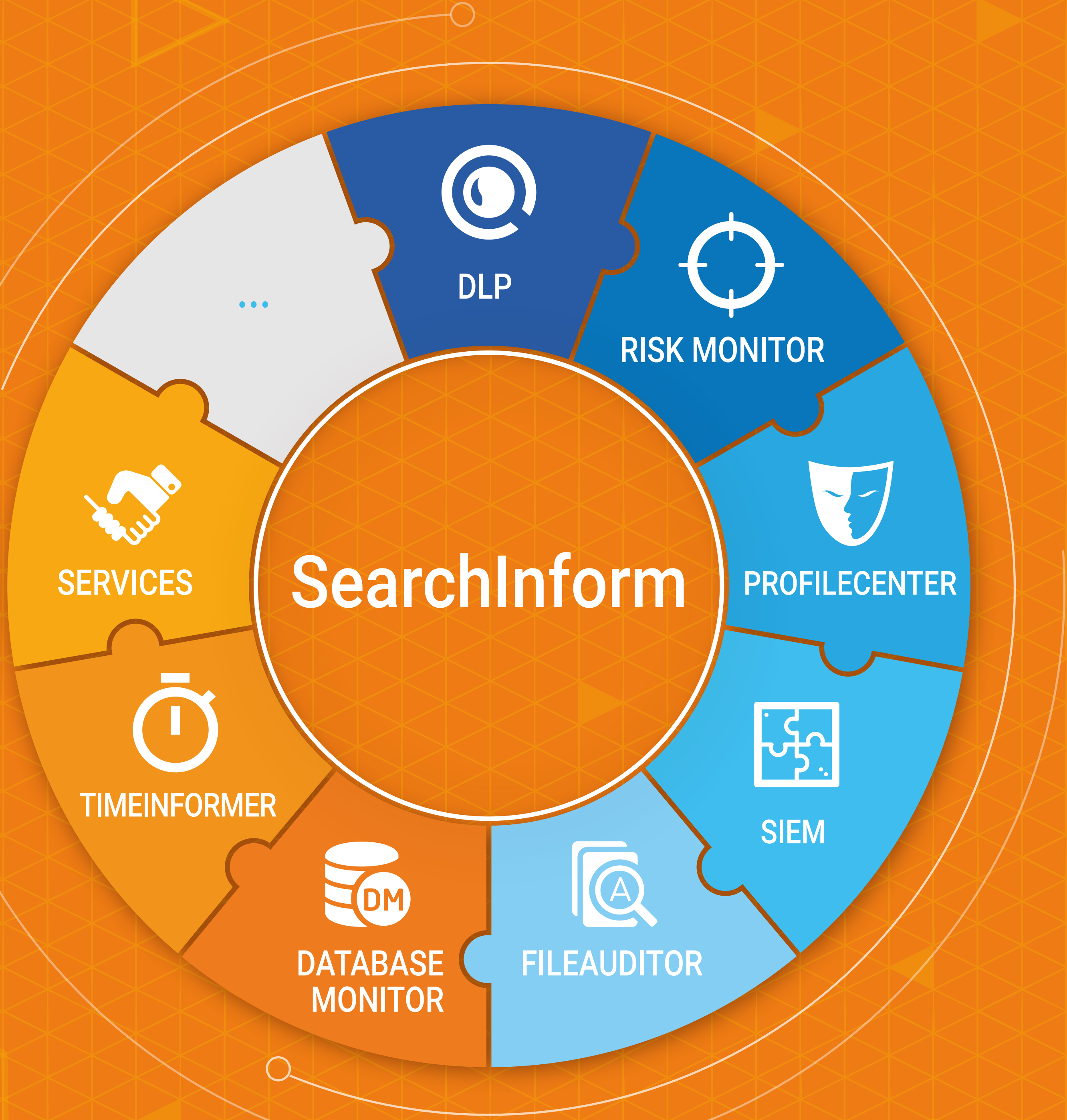
SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INTERNAL THREAT MITIGATION PLATFORM



www.searchinform.com

1995

The company was founded

Moscow, Russia

head office

2 000 000+

computers protected by SearchInform solution

Offices and partners all over the world

3 000+ clients in 20+ countries

8 Products and services for comprehensive data protection

2019 SearchInform started to provide monitoring

Services

2020 SearchInform

solution in the cloud

was announced

32 criminal trials against insiders won by clients

2017 SearchInform software included in

Gartner Magic Quadrant

2018-2020

The Road Show SearchInform

series were held

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

2010

Training Center

was opened

The Radicati Group included SearchInform into the

“Enterprise Data Loss Prevention Market, 2017-2021” study

PRODUCTS AND SERVICES

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

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, their offices are 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

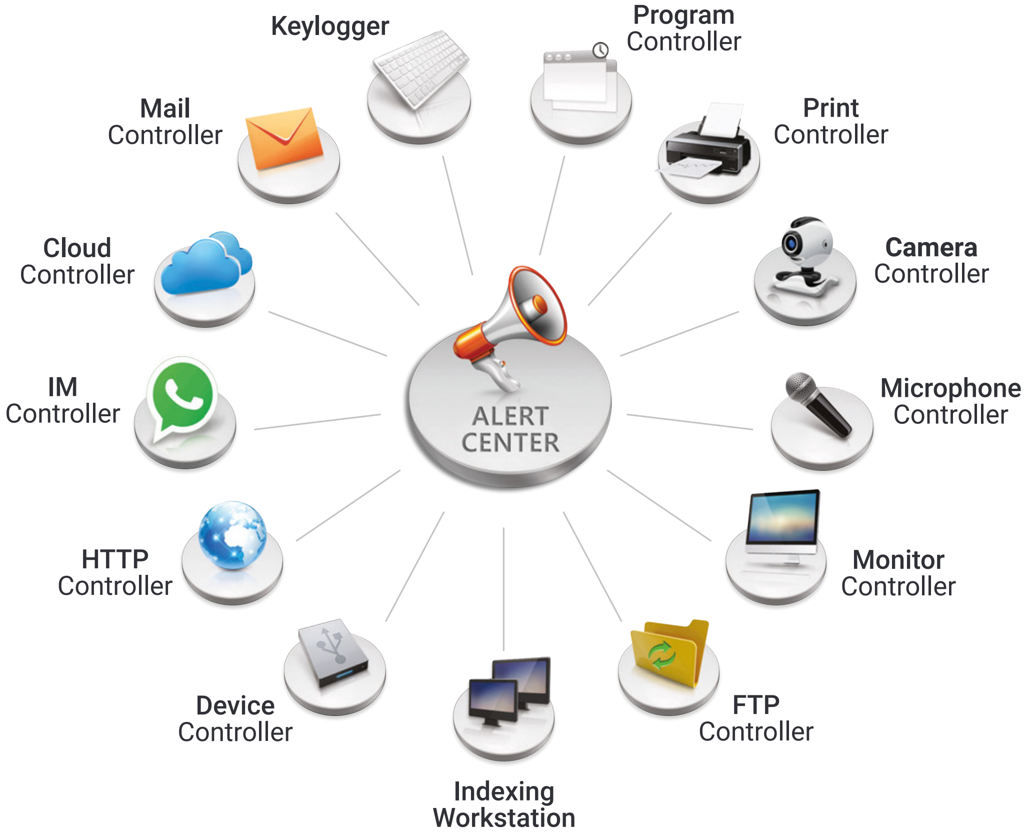
Creates an archive of intercepted information, which facilitates regulatory compliance and security policies enhancement to minimize risks

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.

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 Facebook, Google+, LinkedIn, etc.

Indexing Workstations

Detects confidential documents, which are stored with violations of security policies in shared folders (Shares), computer hard drives (Local System), cloud storages and local NAS systems, on the SharePoint platform.

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.

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.

*****_Helps you monitor remote employee performance_

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

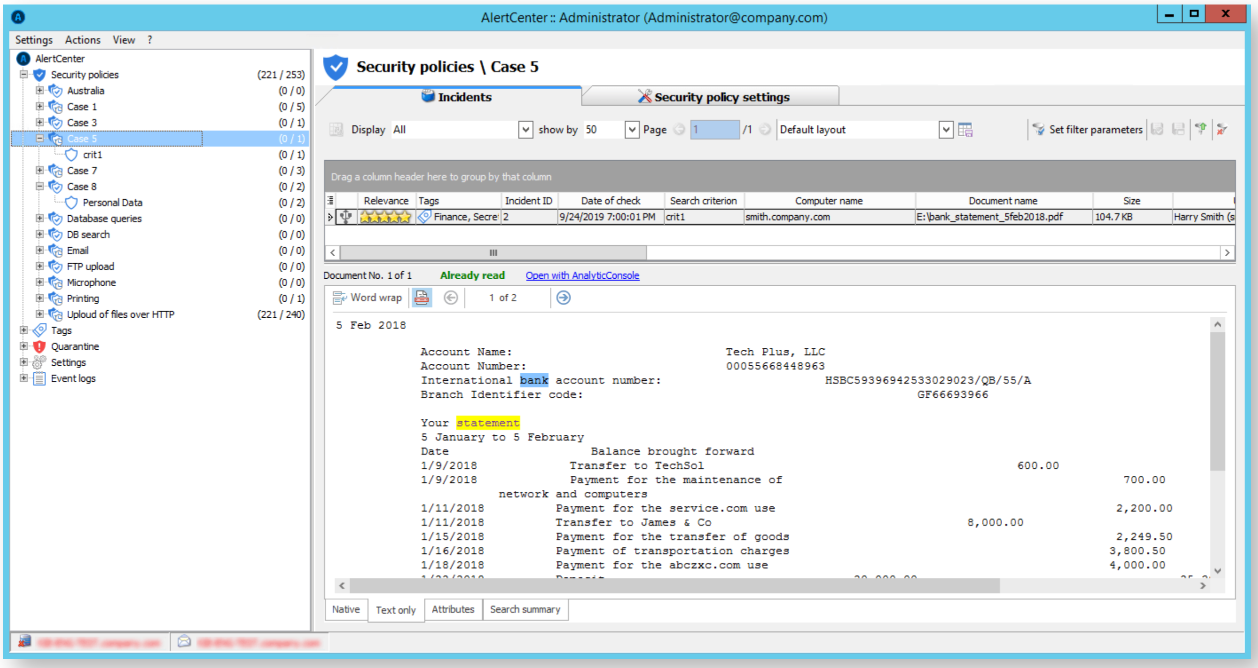
DataCenter

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.



- AlertCenter
  - Security policies (221 / 253)
    - Australia (0 / 0)
    - Case 1 (0 / 5)
    - Case 3 (0 / 1)
    - Case 5 (0 / 1)
      - crit1 (0 / 1)
    - Case 7 (0 / 3)
    - Case 8 (0 / 2)
      - Personal Data (0 / 2)
    - Database queries (0 / 0)
    - DB search (0 / 0)
    - Email (0 / 0)
    - FTP upload (0 / 0)
    - Microphone (0 / 0)
    - Printing (0 / 1)
    - Uploud of files over HTTP (221 / 240)
  - Tags
  - Quarantine
  - Settings
  - Event logs

Security policies \ Case 5

Display All · show by 50 · Page 1 /1 · Default layout · Set filter parameters

Drag a column header here to group by that column

Relevance	Tags	Incident ID	Date of check	Search criterion	Computer name	Document name	Size	
★★★★★	Finance, Secre	2	9/24/2019 7:00:01 PM	crit1	smith.company.com	E:\bank_statement_5feb2018.pdf	104.7 KB	Harry Smith (s

Document No. 1 of 1 · Already read · Open with AnalyticConsole

Word wrap · 1 of 2

```
5 Feb 2018

            Account Name:                          Tech Plus, LLC
            Account Number:                        00055668448963
            International bank account number:                 HSBC59396942533029023/QB/55/A
            Branch Identifier code:                                         GF66693966

            Your statement
            5 January to 5 February
            Date                    Balance brought forward
            1/9/2018                  Transfer to TechSol                                  600.00
            1/9/2018                  Payment for the maintenance of                                     700.00
                       network and computers
            1/11/2018               Payment for the service.com use                                    2,200.00
            1/11/2018               Transfer to James & Co                             8,000.00
            1/15/2018               Payment for the transfer of goods                                  2,249.50
            1/16/2018               Payment of transportation charges                                  3,800.50
            1/18/2018               Payment for the abczxc.com use                                     4,000.00
```

[redacted] [redacted]

Security policies and search results in AlertCenter

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.

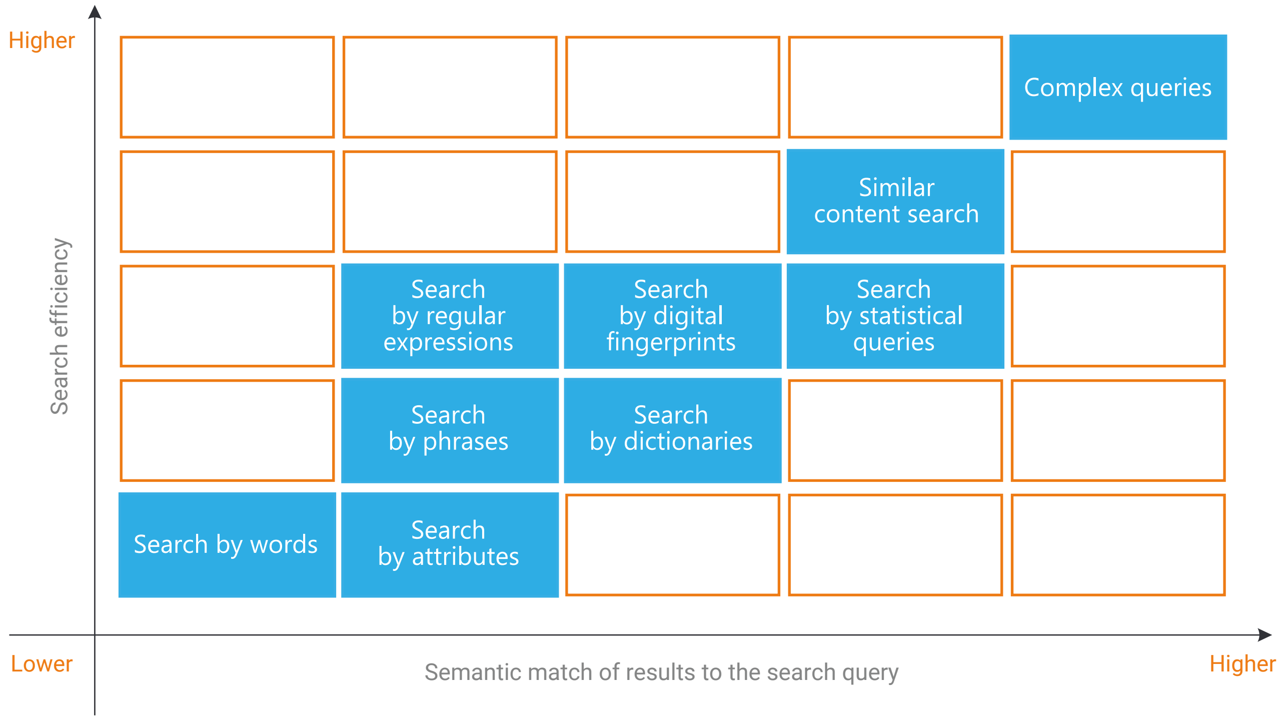
The reports created in Analytic Console are available in the web version of the console.

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. 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

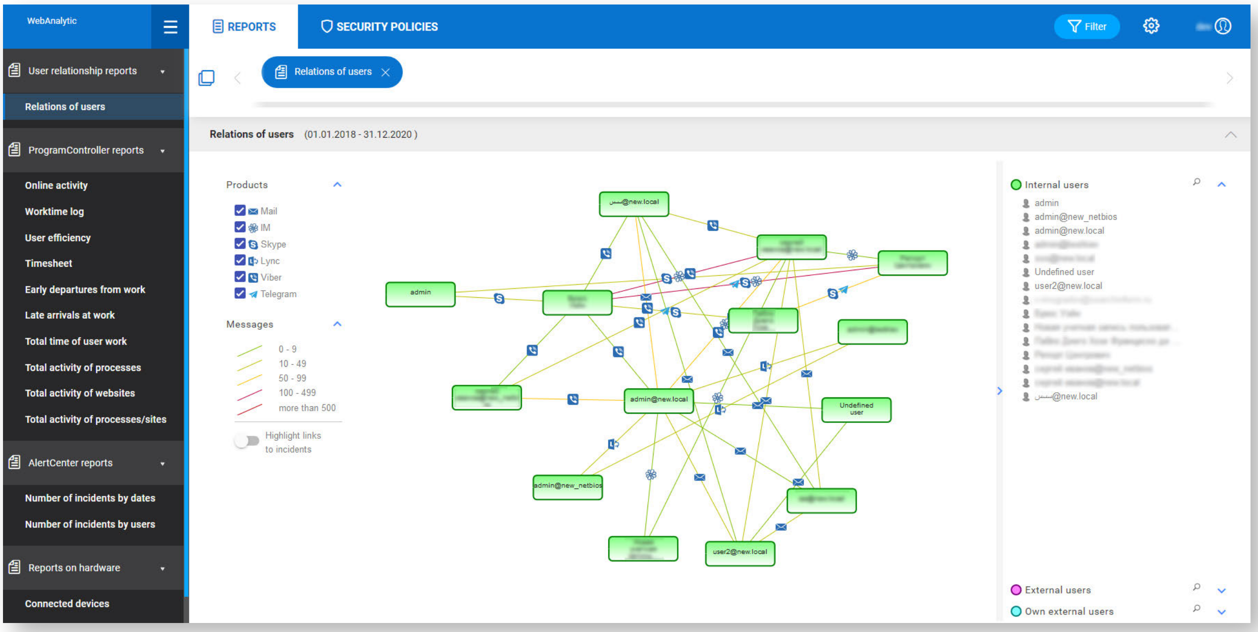
SearchInform solution converts audio records into text and checks whether a transcript complies with the security policies. The system has an option to turn on audio recording when speech is detected or when certain processes or programs, as specified under the relevant security policy, are launched.

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

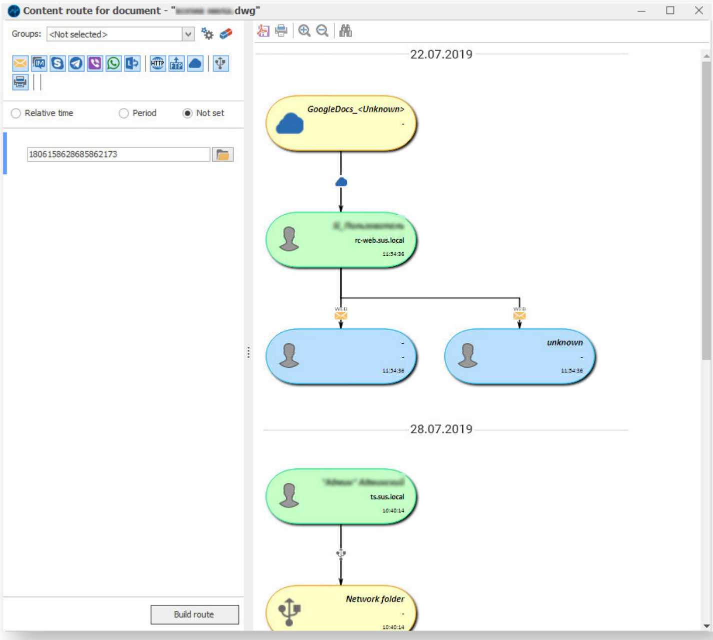
Demonstrates employee-to-employee and employee-to-third-party connections in the form of a relational graph. Visualizes user activities across all communication channels or within a particular communication line. Facilitates corporate investigations.



Analytic Console relational graph

Content routing report

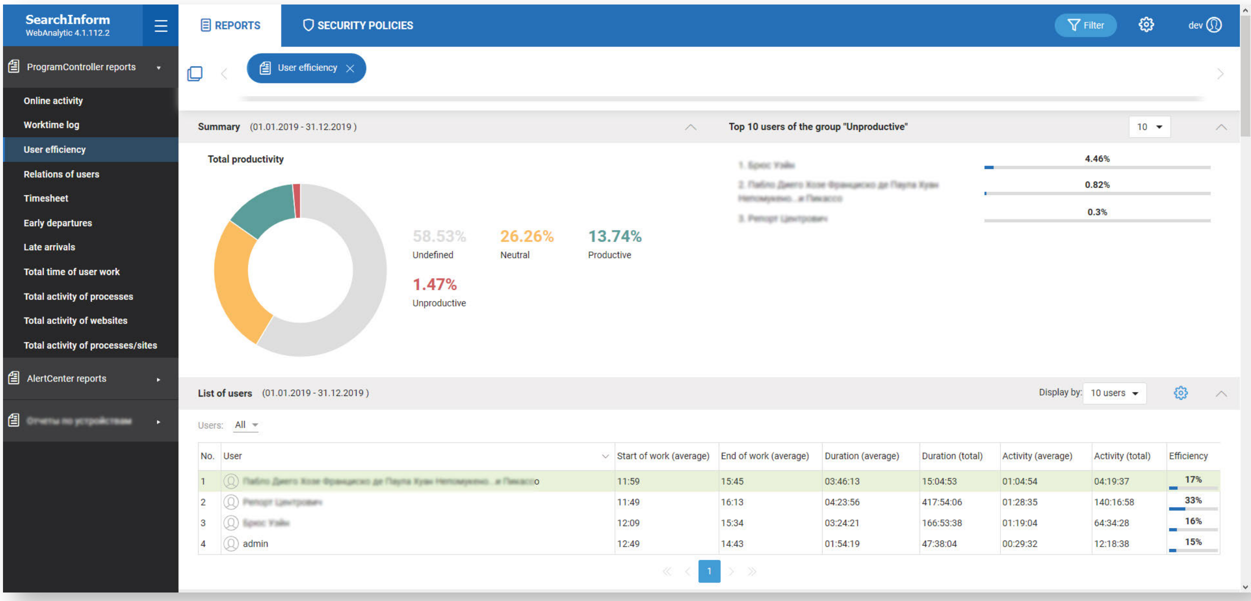
Makes all the document movements between the sender and the recipient via internal and external communication channels completely transparent. Provides for prompt identification of the document's author as well as the source of the respective information and the paths of its distribution.



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.



Summary (01.01.2019 - 31.12.2019)

Top 10 users of the group "Unproductive" 10

1. [redacted]	4.46%
2. [redacted]	0.82%
3. [redacted]	0.3%

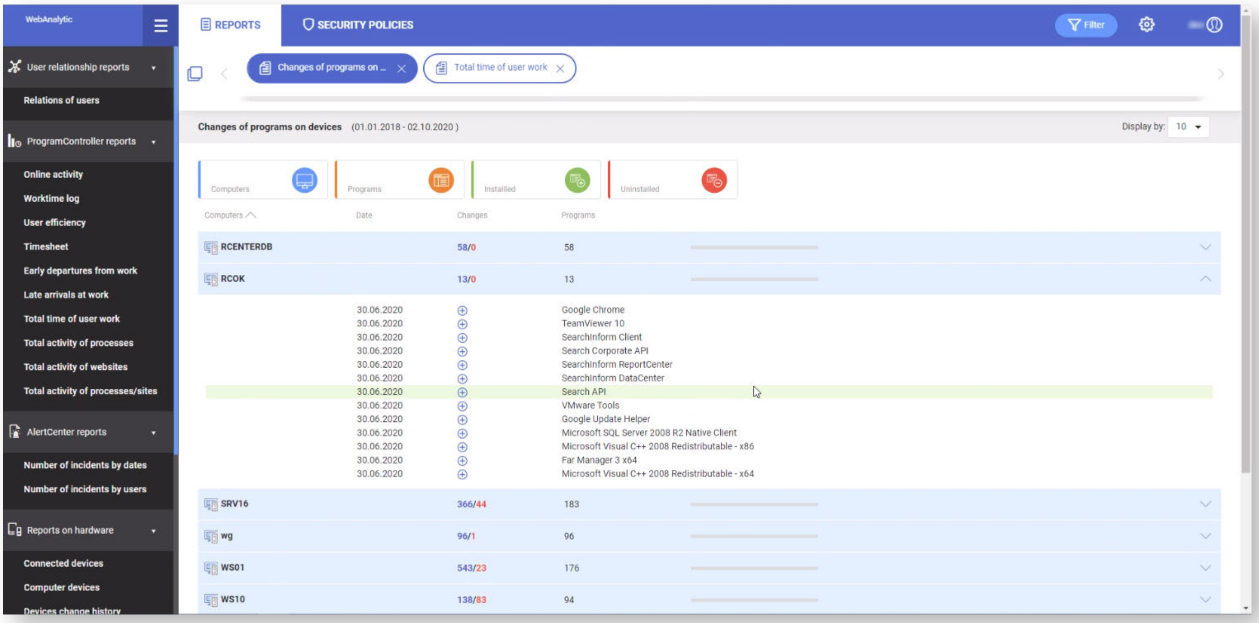
List of users (01.01.2019 - 31.12.2019)

No.	User	Start of work (average)	End of work (average)	Duration (average)	Duration (total)	Activity (average)	Activity (total)	Efficiency
1	[redacted]	11:59	15:45	03:46:13	15:04:53	01:04:54	04:19:37	17%
2	[redacted]	11:49	16:13	04:23:56	417:54:06	01:28:35	140:16:58	33%
3	[redacted]	12:09	15:34	03:24:21	166:53:38	01:19:04	64:34:28	16%
4	admin	12:49	14:43	01:54:19	47:38:04	00:29:32	12:18:38	15%

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 organize data on software installation and uninstallation operations.



Changes of programs on devices (01.01.2018 - 02.10.2020)

Computers	Date	Changes	Programs
RCENTERDB		58/0	58
RCOK		13/0	13
	30.06.2020	⊕	Google Chrome
	30.06.2020	⊕	TeamViewer 10
	30.06.2020	⊕	SearchInform Client
	30.06.2020	⊕	Search Corporate API
	30.06.2020	⊕	SearchInform ReportCenter
	30.06.2020	⊕	SearchInform DataCenter
	30.06.2020	⊕	Search API
	30.06.2020	⊕	VMware Tools
	30.06.2020	⊕	Google Update Helper
	30.06.2020	⊕	Microsoft SQL Server 2008 R2 Native Client
	30.06.2020	⊕	Microsoft Visual C++ 2008 Redistributable - x86
	30.06.2020	⊕	Far Manager 3 x64
	30.06.2020	⊕	Microsoft Visual C++ 2008 Redistributable - x64
SRV16		366/44	183
wg		96/1	96
WS01		543/23	176
WS10		138/83	94

Software and hardware report

ADVANTAGES

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.

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.

Tools for step-by-step incident investigations

Recording conversations and capturing onscreen content in real time, monitoring keyboard inputs and making video with a webcam – the system’s integrated components help trace back the violation step by step.

Cloud deployment model

Al 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.

Visualization of connections between employees

An interactive relational graph is a good visual aid demonstrating social circles and communication lines involving both the company’s employees and their third-party contact persons.

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).

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.

Comprehensive solution

The multi-component structure will provide you with adequate solutions whether you would like to pursue comprehensive multiple-channel monitoring of data leakages or just combine a number of modules of your choice based on your needs – in which case the cost will be significantly lower.

Security safeguards for geographically dispersed companies

In remote branch offices with a small number of PCs and a ‘narrowband’ communication channel to the head office, where it is impracticable to deploy a full-fledged system, data will be filtered, processed and encrypted locally before being transferred to the server.

Control agents for OS Linux

SearchInform product can run under some of the most popular distros.

Integration with other SearchInform products

SearchInform solution is seamlessly integrated with SIEM, ProfileCenter, FileAuditor and Database Monitor, 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.

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.

An archive of intercepted information

Significantly facilitates event chain reconstruction and allows a company to conduct retrospective investigation.

Data at rest monitoring

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

SearchInform ProfileCenter

74% of companies found out that their employees do non-work related activities during work hours*

74%
INCIDENTS

*According to the SearchInform solution implementation statistics 2019

A company's objective is to simulate a risk, foresee employee activity and prevent an incident.

The problem is solved by ProfileCenter – the non-test diagnostics toolset which helps to classify personalities, forecast behavior, highlight strengths and weaknesses and detect criminal propensity.

HOW CAN PROFILING HELP BUSINESSES?

Profiling methods are applied in business to disclose fraudulent activity, enhance personnel management techniques, increase sales and assess risks caused by personality traits which can harm colleagues or a company.

ProfileCenter detects:

- Propensity to commit a crime
- Key personality traits, strengths and weaknesses
- Behavior in conflict situations
- Employee social role within a team
- Hidden attitudes
- Basic emotions

HOW DOES THE PRODUCT WORK?

STEP 1

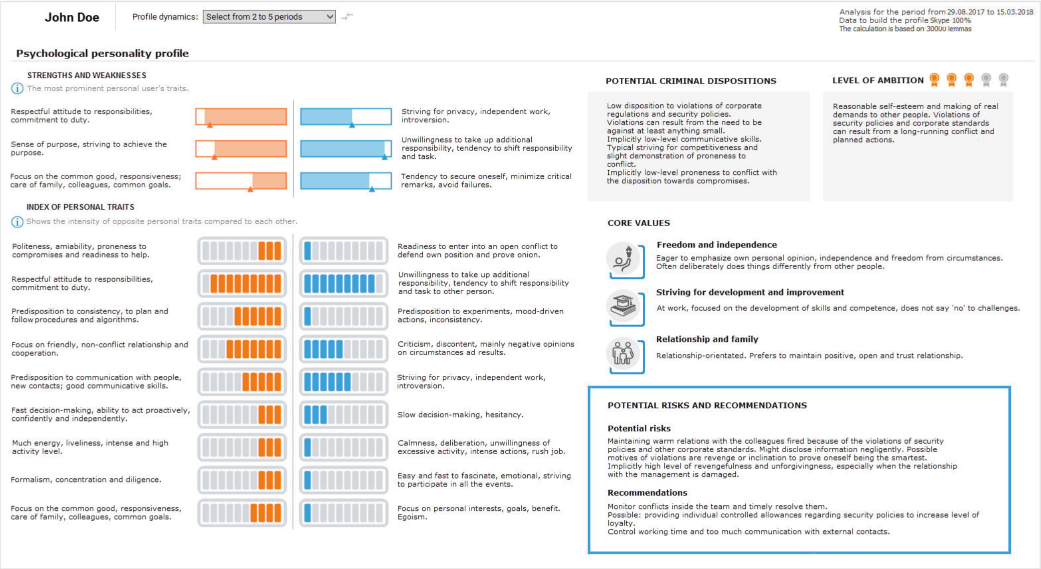
The system collects employees' correspondence (email, messengers, social media)

STEP 2

The software performs behavior peculiarities and thinking patterns identification based on the text analysis featuring 70+ criteria

STEP 3

The results of the analysis are displayed as a report with a commentary and hands-on approach



John Doe

Profile dynamics: Select from 2 to 5 periods

Analysis for the period from 29.08.2017 to 15.03.2018
Data to build the profile Skype 100%
The calculation is based on 30000 lemmas

Psychological personality profile

STRENGTHS AND WEAKNESSES

The most prominent personal user's traits.

Respectful attitude to responsibilities, commitment to duty.	Striving for privacy, independent work, introversion.
Sense of purpose, striving to achieve the purpose.	Unwillingness to take up additional responsibility, tendency to shift responsibility and task.
Focus on the common good, responsiveness; care of family, colleagues, common goals.	Tendency to secure oneself, minimize critical remarks, avoid failures.

INDEX OF PERSONAL TRAITS

Shows the intensity of opposite personal traits compared to each other.

Politeness, amiability, proneness to compromises and readiness to help.	Readiness to enter into an open conflict to defend own position and prove onion.
Respectful attitude to responsibilities, commitment to duty.	Unwillingness to take up additional responsibility, tendency to shift responsibility and task to other person.
Predisposition to consistency, to plan and follow procedures and algorithms.	Predisposition to experiments, mood-driven actions, inconsistency.
Focus on friendly, non-conflict relationship and cooperation.	Criticism, discontent, mainly negative opinions on circumstances ad results.
Predisposition to communication with people, new contacts; good communicative skills.	Striving for privacy, independent work, introversion.
Fast decision-making, ability to act proactively, confidently and independently.	Slow decision-making, hesitancy.
Much energy, liveliness, intense and high activity level.	Calmness, deliberation, unwillingness of excessive activity, intense actions, rush job.
Formalism, concentration and diligence.	Easy and fast to fascinate, emotional, striving to participate in all the events.
Focus on the common good, responsiveness, care of family, colleagues, common goals.	Focus on personal interests, goals, benefit. Egoism.

POTENTIAL CRIMINAL DISPOSITIONS

Low disposition to violations of corporate regulations and security policies.
Violations can result from the need to be against at least anything small.
Implicitly low-level communicative skills.
Typical striving for competitiveness and slight demonstration of proneness to conflict.
Implicitly low-level proneness to conflict with the disposition towards compromises.

LEVEL OF AMBITION

Reasonable self-esteem and making of real demands to other people. Violations of security policies and corporate standards can result from a long-running conflict and planned actions.

CORE VALUES

Freedom and independence
Eager to emphasize own personal opinion, independence and freedom from circumstances. Often deliberately does things differently from other people.

Striving for development and improvement
At work, focused on the development of skills and competence, does not say 'no' to challenges.

Relationship and family
Relationship-orientated. Prefers to maintain positive, open and trust relationship.

POTENTIAL RISKS AND RECOMMENDATIONS

Potential risks
Maintaining warm relations with the colleagues fired because of the violations of security policies and other corporate standards. Might disclose information negligently. Possible motives of violations are revenge or inclination to prove oneself being the smartest.
Implicitly high level of revengefulness and unforgivingness, especially when the relationship with the management is damaged.

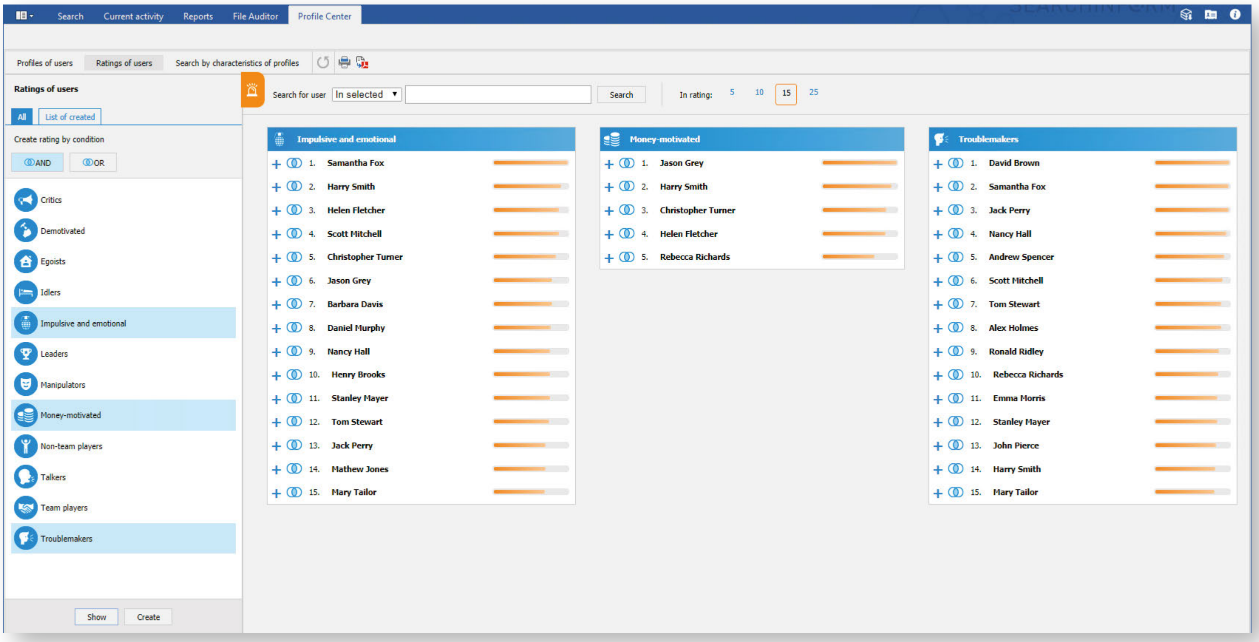
Recommendations
Monitor conflicts inside the team and timely resolve them.
Possible: providing individual controlled allowances regarding security policies to increase level of loyalty.
Control working time and too much communication with external contacts.

Personal profile of an employee

THE PRODUCT FACILITATES DECISION MAKING

Receive practical recommendations on:

- Which employee behavior patterns should draw your attention
- How to create an efficient team
- Who should be monitored sometimes and who – always or in specific situations
- How safe is it to give access to confidential information, financial assets and valuable sources
- Whether a job is suitable for an employee
- Who should be communicated with officially and businesslike and who is open to establish friendship
- Whether a reprimand or short instruction is a sufficient measure or some employees need to be systematically trained or even penalized



Impulsive and emotional
1. Samantha Fox
2. Harry Smith
3. Helen Fletcher
4. Scott Mitchell
5. Christopher Turner
6. Jason Grey
7. Barbara Davis
8. Daniel Murphy
9. Nancy Hall
10. Henry Brooks
11. Stanley Mayer
12. Tom Stewart
13. Jack Perry
14. Mathew Jones
15. Mary Tailor

Money-motivated
1. Jason Grey
2. Harry Smith
3. Christopher Turner
4. Helen Fletcher
5. Rebecca Richards

Troublemakers
1. David Brown
2. Samantha Fox
3. Jack Perry
4. Nancy Hall
5. Andrew Spencer
6. Scott Mitchell
7. Tom Stewart
8. Alex Holmes
9. Ronald Ridley
10. Rebecca Richards
11. Emma Morris
12. Stanley Mayer
13. John Pierce
14. Harry Smith
15. Mary Tailor

User rating

ADVANTAGES

- Automated solution provides you with results promptly and saves money on hiring a profiler
- Analyzes data collected by a data protection solution, the relevance of which is higher than that obtained during open testing
- Monitors personality in dynamics
- Doesn’t distract staff from work, and doesn’t escalate the situation
- Detects changes in moods and attitudes within a team

SearchInform SIEM

- FIRST OUT-OF-THE-BOX SIEM
- POLICY CREATION IN TWO CLICKS

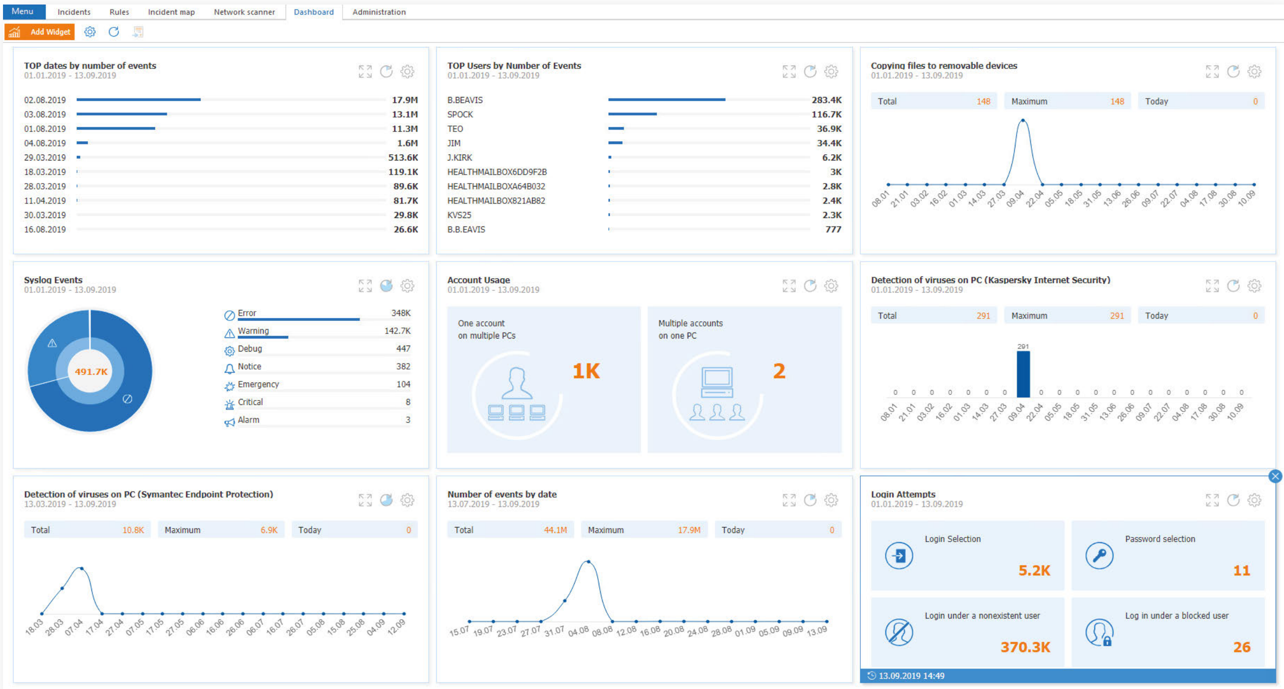
No. 1

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 need 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.



TOP dates by number of events
01.01.2019 - 13.09.2019

02.08.2019	17.9M
03.08.2019	13.1M
01.08.2019	11.3M
04.08.2019	1.6M
29.03.2019	513.6K
18.03.2019	119.1K
28.03.2019	89.6K
11.04.2019	81.7K
30.03.2019	29.8K
16.08.2019	26.6K

TOP Users by Number of Events
01.01.2019 - 13.09.2019

B.BEAVIS	283.4K
SPOCK	116.7K
TEO	36.9K
JIM	34.4K
J.KIRK	6.2K
HEALTHMAILBOX6DD9F2B	3K
HEALTHMAILBOXA64B032	2.8K
HEALTHMAILBOX821AB82	2.4K
KVS25	2.3K
B.B.EAVIS	777

Copying files to removable devices
01.01.2019 - 13.09.2019

Total 148 Maximum 148 Today 0

Syslog Events
01.01.2019 - 13.09.2019

Error	348K
Warning	142.7K
Debug	447
Notice	382
Emergency	104
Critical	8
Alarm	3

Account Usage
01.01.2019 - 13.09.2019

One account on multiple PCs 1K

Multiple accounts on one PC 2

Detection of viruses on PC (Kaspersky Internet Security)
01.01.2019 - 13.09.2019

Total 291 Maximum 291 Today 0

Detection of viruses on PC (Symantec Endpoint Protection)
13.03.2019 - 13.09.2019

Total 10.8K Maximum 6.9K Today 0

Number of events by date
13.07.2019 - 13.09.2019

Total 44.1M Maximum 17.9M Today 0

Login Attempts
01.01.2019 - 13.09.2019

Login Selection 5.2K

Password selection 11

Login under a nonexistent user 370.3K

Log in under a blocked user 26

13.09.2019 14:49

Event statistics dashboard

SearchInform SIEM reveals:

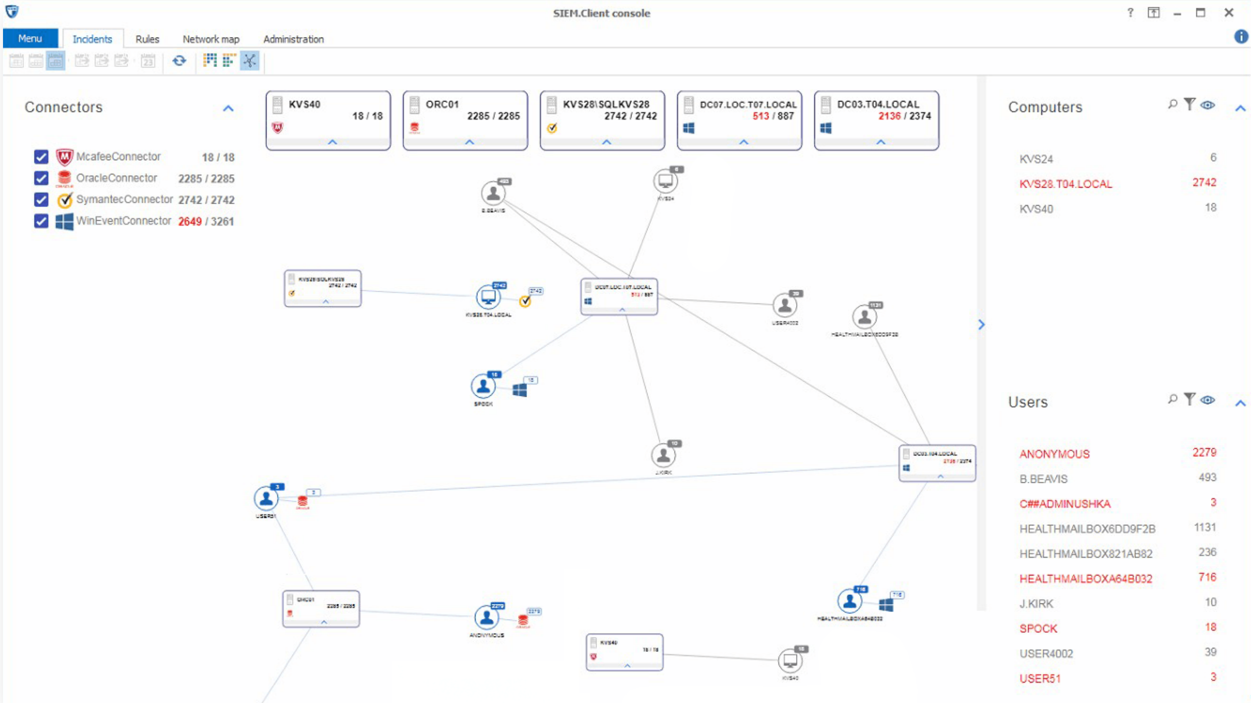
- Virus epidemics and separate infections
- Attempts to gain unauthorized access to data
- Account password guessing
- Active accounts of dismissed employees that had to be deleted
- Hardware configuration errors
- Permissible operating temperature abuse
- Data removal from critical resources
- Use of 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

PRESET SECURITY POLICIES

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 your own policies (user connector function).

- 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.



Connectors

☑ McafeeConnector	18 / 18
☑ OracleConnector	2285 / 2285
☑ SymantecConnector	2742 / 2742
☑ WinEventConnector	2649 / 3261

Computers

KVS24	6
KVS28.T04.LOCAL	2742
KVS40	18

Users

ANONYMOUS	2279
B.BEAVIS	493
C##ADMINUSHKA	3
HEALTHMAILBOX6DD9F2B	1131
HEALTHMAILBOX821AB82	236
HEALTHMAILBOXA64B032	716
J.KIRK	10
SPOCK	18
USER4002	39
USER51	3

Incident display screen

ADVANTAGES

- Quick implementation without intensive preliminary configuration, the software can start working on the installation day
- Integration with SearchInform products increases the level of information security of a company and makes it possible to fully investigate the incident and collect evidence base
- Easy-to-use system, a specialist without IT skills will cope with the program as it doesn’t require knowledge of programming languages to create correlation and cross correlation rules
- Low hardware and software requirements and reasonable price even for small-sized business

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 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.

FileAuditor solves the following tasks:

Classification of vulnerable data

Finds files in a document flow that contain critical information, and assigns a certain type to each file: personal data, trade secret, credit card numbers, etc.

Critical documents archiving

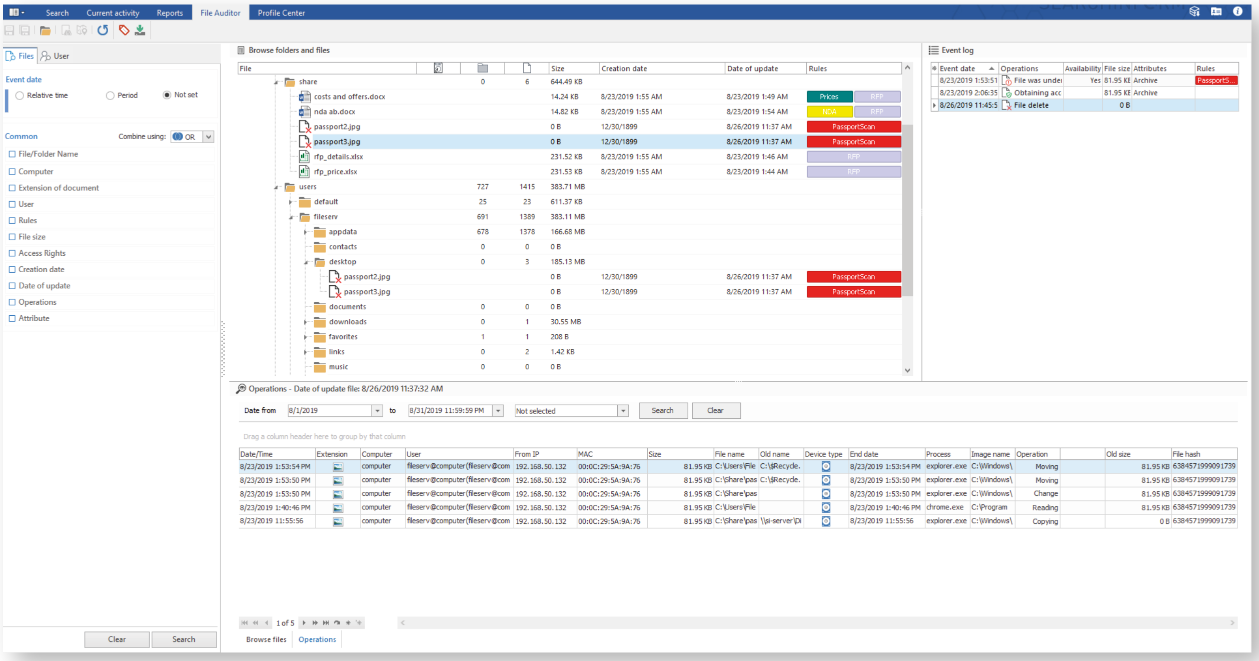
Makes shadow copies of critical files found on a PC, server or network folders, saves the history of their revisions. Confidential data archive helps in incident investigation and ensures recovery of lost information.

Access rights audit

Facilitates confidential information access control – automatically monitors open resources, files available to a specific user or group, privileged accounts.

User activity monitoring

Audits user operations in a file system and their chronology. The specialists responsible for risk mitigation always have their information about changes made to a file updated (creating, editing, moving, deleting, etc.).



Event date

○ Relative time ○ Period ● Not set

Common

Combine using: OR

□ File/Folder Name
□ Computer
□ Extension of document
□ User
□ Rules
□ File size
□ Access Rights
□ Creation date
□ Date of update
□ Operations
□ Attribute

Browse folders and files

File				Size	Creation date	Date of update	Rules
share		0	6	644.49 KB			
costs and offers.docx				14.24 KB	8/23/2019 1:55 AM	8/23/2019 1:49 AM	Prices RFP
nda ab.docx				14.82 KB	8/23/2019 1:55 AM	8/23/2019 1:54 AM	NDA RFP
passport2.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	PassportScan
passport3.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	PassportScan
rfp_details.xlsx				231.52 KB	8/23/2019 1:55 AM	8/23/2019 1:46 AM	RFP
rfp_price.xlsx				231.53 KB	8/23/2019 1:55 AM	8/23/2019 1:44 AM	RFP
users		727	1415	383.71 MB			
default		25	23	611.37 KB			
fileserv		691	1389	383.11 MB			
appdata		678	1378	166.68 MB			
contacts		0	0	0 B			
desktop		0	3	185.13 MB			
passport2.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	PassportScan
passport3.jpg				0 B	12/30/1899	8/26/2019 11:37 AM	PassportScan
documents		0	0	0 B			
downloads		0	1	30.55 MB			
favorites		1	1	208 B			
links		0	2	1.42 KB			
music		0	0	0 B			

Event log

Event date	Operations	Availability	File size	Attributes	Rules
8/23/2019 1:53:51	File was under	Yes	81.95 KB	Archive	PassportS...
8/23/2019 2:06:35	Obtaining acc		81.95 KB	Archive	
8/26/2019 11:45:5	File delete		0 B		

Operations - Date of update file: 8/26/2019 11:37:32 AM

Date from 8/1/2019 to 8/31/2019 11:59:59 PM Not selected

Drag a column header here to group by that column

Date/Time	Extension	Computer	User	From IP	MAC	Size	File name	Old name	Device type	End date	Process	Image name	Operation		Old size	File hash
8/23/2019 1:53:54 PM		computer	fileserv@computer(fileserv@com	192.168.50.132	00:0C:29:5A:9A:76	81.95 KB	C:\Users\File	C:\$Recycle.		8/23/2019 1:53:54 PM	explorer.exe	C:\Windows\	Moving		81.95 KB	6384571999091739
8/23/2019 1:53:50 PM		computer	fileserv@computer(fileserv@com	192.168.50.132	00:0C:29:5A:9A:76	81.95 KB	C:\Share\pas	C:\$Recycle.		8/23/2019 1:53:50 PM	explorer.exe	C:\Windows\	Moving		81.95 KB	6384571999091739
8/23/2019 1:53:50 PM		computer	fileserv@computer(fileserv@com	192.168.50.132	00:0C:29:5A:9A:76	81.95 KB	C:\Share\pas			8/23/2019 1:53:50 PM	explorer.exe	C:\Windows\	Change		81.95 KB	6384571999091739
8/23/2019 1:40:46 PM		computer	fileserv@computer(fileserv@com	192.168.50.132	00:0C:29:5A:9A:76	81.95 KB	C:\Users\File			8/23/2019 1:40:46 PM	chrome.exe	C:\Program	Reading		81.95 KB	6384571999091739
8/23/2019 11:55:56		computer	fileserv@computer(fileserv@com	192.168.50.132	00:0C:29:5A:9A:76	81.95 KB	C:\Share\pas	\\si-server\Di		8/23/2019 11:55:56	explorer.exe	C:\Windows\	Copying		0 B	6384571999091739

Audit of a file containing confidential information

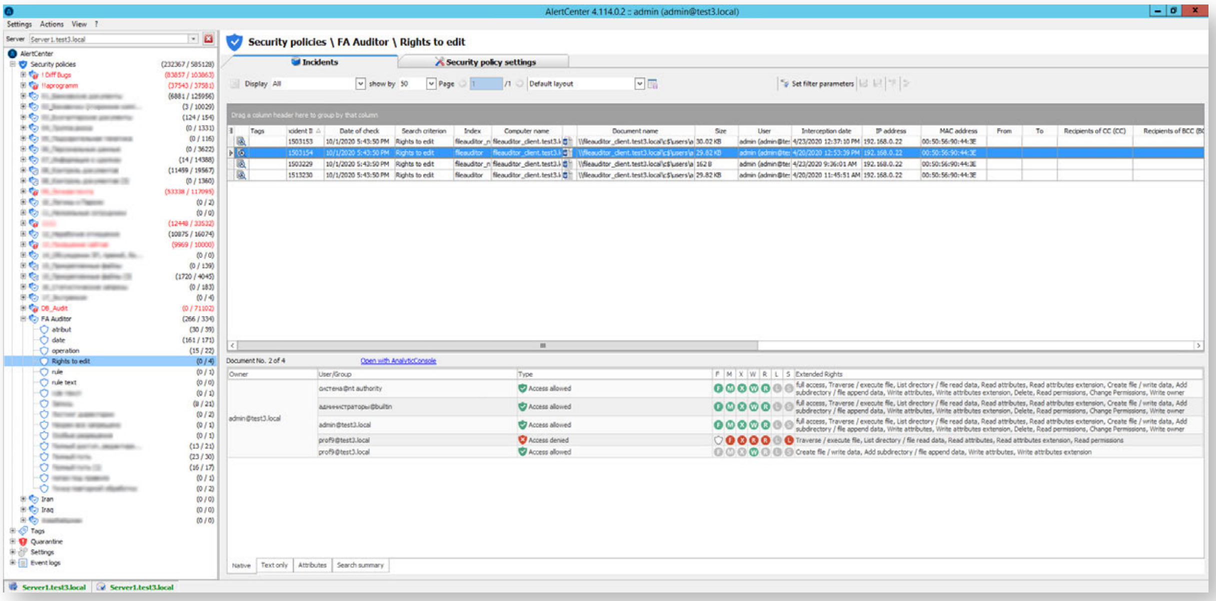
DATA ANALYSIS

FileAuditor analytical module visualizes results of scanning a file system in accordance with set rules. Rule settings have different search types available (by content, attributes, regular expressions, dictionaries). 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 with indication of 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.



Security policies \ FA Auditor \ Rights to edit

Display: All | show by: 50 | Page 1 /1 | Default layout

Tags	ncident №	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 (BC
	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

Owner	User/Group	Type	F	M	X	W	R	L	S	Extended Rights
admin@test3.local	система@nt authority	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
	администраторы@builtin	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

Folder tree with marking of sensitive documents

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.

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; storage of only sensitive documents is possible; a deduplication system saves storage space
- Customizable rule settings save specialists from unnecessary work, allowing them to 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

SearchInform Database Monitor

SearchInform Database Monitor is a DAM (Database Activity Monitoring) solution for automated monitoring and audit of operations on databases and in business applications.

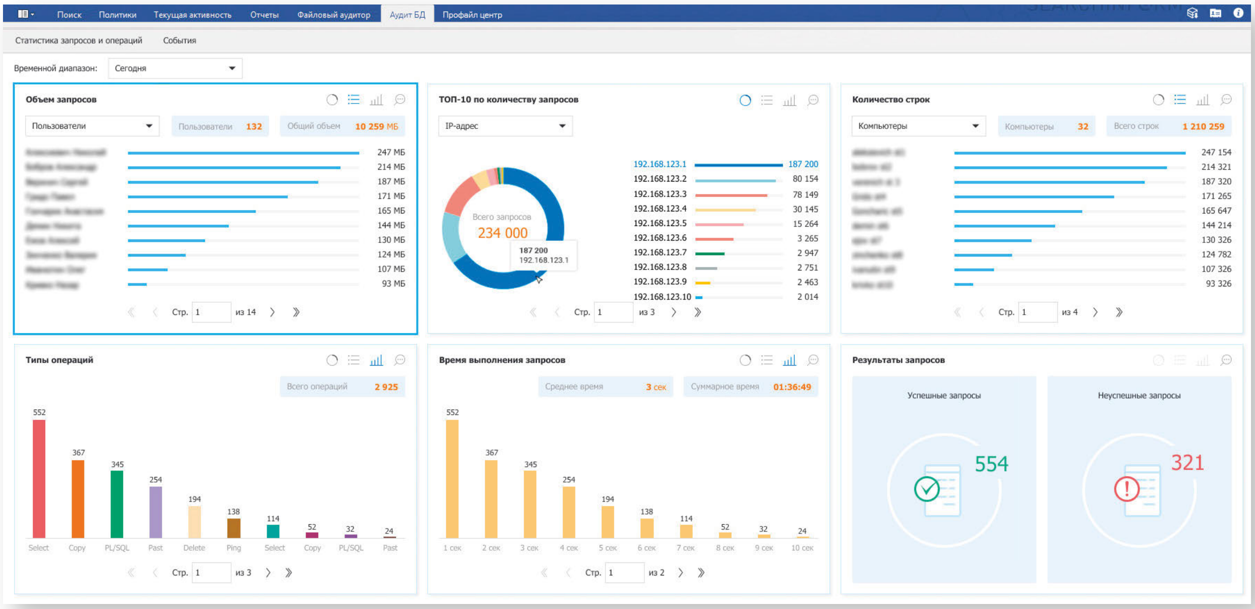
A company's security system is affected not only by data leakage outside the perimeter, but also by information modification inside corporate databases. For example: an employee modified information in CRM or changed a phone number linked to a client’s bank account; an employee is trying to unload a large amount of data from CRM or, vice versa, is trying to delete details. These situations are as important as information leakage consequences.

HOW DOES THE SOLUTION WORK?

Database Monitor logs all database queries and responses. The solution analyzes the information collected in accordance with the specified rules – security policies. In case of violation, the system notifies the specialists responsible for risk mitigation within an organization. Database Monitor allows the specialists to monitor activity and identify those who access a database and how they use it.

Database Monitor controls:

- Direct database queries (system administrator queries)
- Access to the database via business applications
- Unloading large amount of information from a database
- Unloading of data containing sensitive information (trade secret, personal data, customer databases)
- Database content modification (deleting, editing, etc.)



Database Monitor audit results

ANALYTICAL CAPABILITIES

The product can be compared to a filter through which all user queries and SQL server responses pass. Database Monitor indexes database queries automatically making them available for search and analysis.

The system integrates various types of search algorithms (by phrases, by database and user attributes, by regular expressions, by types of database queries, etc.), which can be combined into complex queries, specifying the search conditions.

SPECIALISTS WILL BE ABLE TO VIEW DATABASE AUDIT REPORTS IN REAL TIME AND REQUEST REPORTS FOR VARIOUS TIME INTERVALS.

Reports demonstrate:

- Query and operation statistics
- Activity of application accounts which have access to a database
- Database queries from users (including critical information queries)
- An account suspicious activity (an abnormally large number of requests, uploading heavy files, etc.)
- Current list of databases

Database Monitor analytic module allows specialists to detect suspicious actions of employees promptly and launch an investigation.

ADVANTAGES

- A wide range of search algorithms, including full-text morphological search for in-depth analysis of indexed queries
- Common criteria (for Risk Monitor and Database Monitor) for creating security policies, which simplifies working with the solution
- Visual presentation of audit results using tables and graphs
- Effective traffic processing (the software analyzes only specified in settings database queries)
- Integration of Database Monitor with other SearchInform products

SearchInform TimeInformer

For some employees being at work does not automatically mean attending to 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 later, 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 under 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.

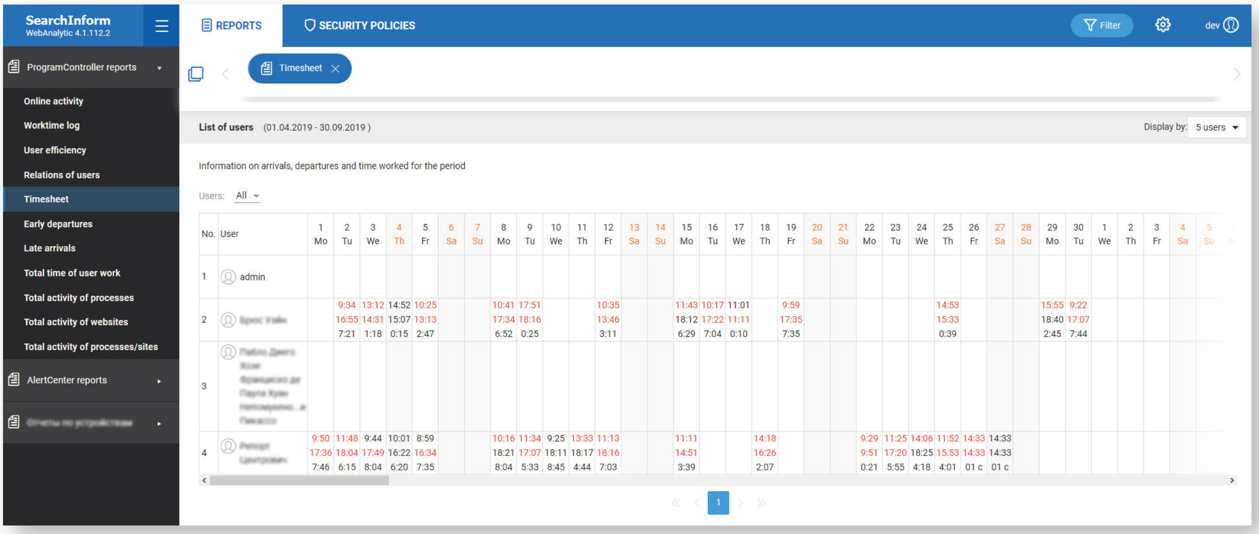
TimeInformer has the following groups of reports:

- 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.



List of users (01.04.2019 - 30.09.2019)

Information on arrivals, departures and time worked for the period

No.	User	1 Mo	2 Tu	3 We	4 Th	5 Fr	6 Sa	7 Su	8 Mo	9 Tu	10 We	11 Th	12 Fr	13 Sa	14 Su	15 Mo	16 Tu	17 We	18 Th	19 Fr	20 Sa	21 Su	22 Mo	23 Tu	24 We	25 Th	26 Fr	27 Sa	28 Su	29 Mo	30 Tu	1 We	2 Th	3 Fr	4 Sa	5 Su
1	admin																																			
2	[redacted]		9:34 16:55 7:21	13:12 14:31 1:18	14:52 15:07 0:15	10:25 13:13 2:47			10:41 17:34 6:52	17:51 18:16 0:25			10:35 13:46 3:11			11:43 18:12 6:29	10:17 17:22 7:04	11:01 11:11 0:10		9:59 17:35 7:35						14:53 15:33 0:39				15:55 18:40 2:45	9:22 17:07 7:44					
3	[redacted]																																			
4	[redacted]	9:50 17:36 7:46	11:48 18:04 6:15	9:44 17:49 8:04	10:01 16:22 6:20	8:59 16:34 7:35			10:16 18:21 8:04	11:34 17:07 5:33	9:25 18:11 8:45	13:33 18:17 4:44	11:13 18:16 7:03			11:11 14:51 3:39			14:18 16:26 2:07				9:29 9:51 0:21	11:25 17:20 5:55	14:06 18:25 4:18	11:52 15:53 4:01	14:33 14:33 01 c	14:33 14:33 01 c								

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

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. Some 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 SIEM	+	-
SearchInform FileAuditor	+	+
SearchInform Database Monitor	+	-
SearchInform TimeInformer	+	+
SearchInform ProfileCenter	+	+

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).

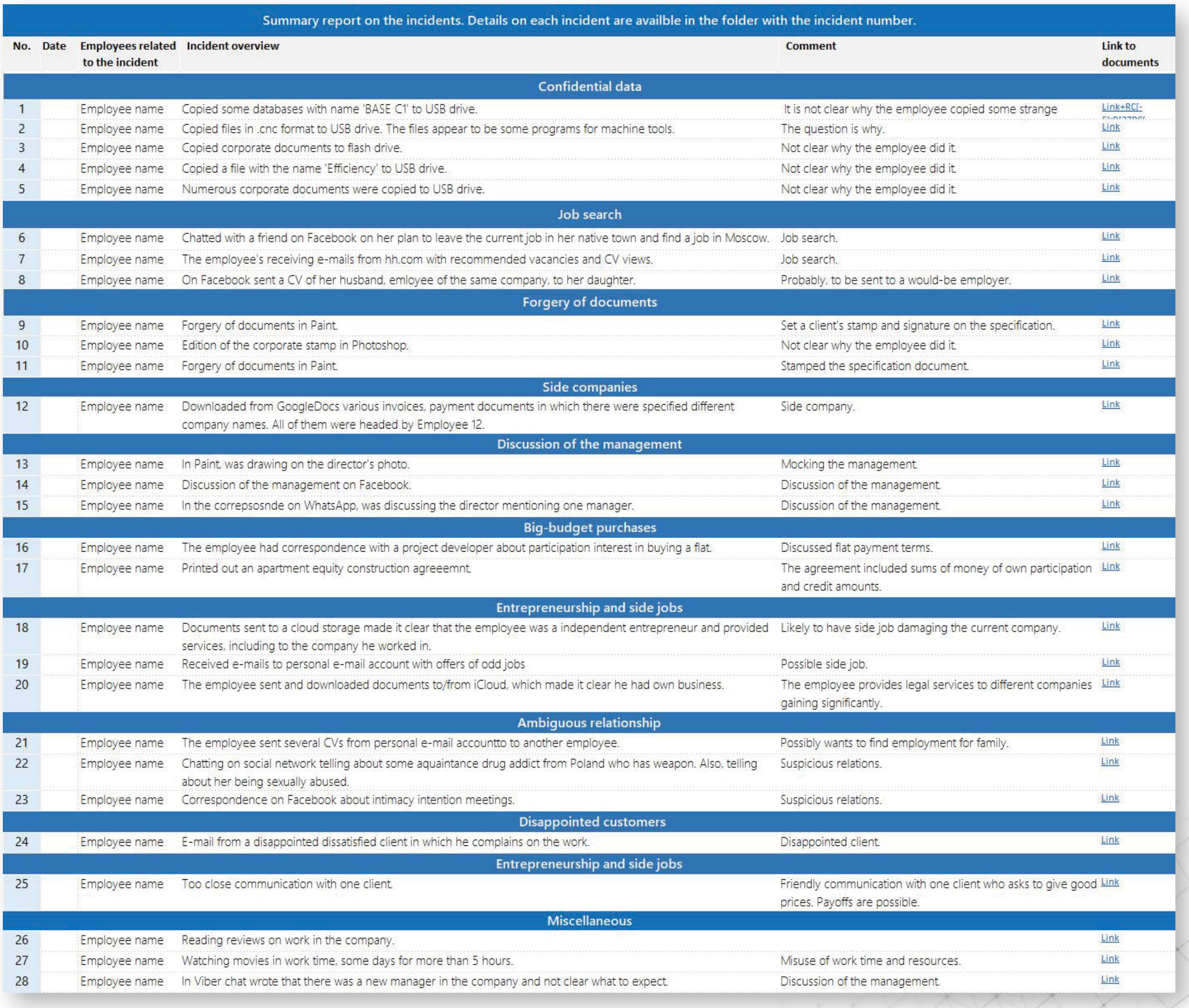
A customer can work with the system together with a specialist or independently.

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+RC[-
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.

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 43 80 19 13
+7925 681 1803
Email: v.prestes@searchinform.com

KAZAKHSTAN

Almaty
Phone: +7 727 239 30 36
+7 727 222 17 95
Email: d.stelchenko@searchinform.ru

MENA

Phone: +375 25 708 77 69
Email: yamen@searchinform.com

RUSSIA

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

SERBIA

Belgrade
Phone: +381 11 45 323 10
+381 69 44 210 44
Email: m.prerad@searchinform.com

SOUTH AFRICA

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

UK

London
Phone: +44 0 20 3808 4340
Email: uk@searchinform.com