SEARCHINFORM

INTERNAL THREAT MITIGATION PLATFORM

searchinform.com

1995 The company was founded

3 000 000+
computers are protected by SearchInform software

4 000+ Clients all over the world

6 products enabling comprehensive data protection against threats

2017

SearchInform software was listed in

Gartner Magic Quadrant

2019

SearchInform started to provide monitoring

Services

2020

SearchInform's

cloud solutions

announced

The Radicati Group

included SearchInform into the

Enterprise Data Loss Prevention Market, 2017-2021 study

2018-2020

The Road Show SearchInform

series were held in

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

2022-2023

+9 North African countries — SearchInform expanded its presence

2023

SearchInform opened local representative office in

Dubai (UAE)

2025

SearchInform opened local representative office in

Riyadh, (KSA)

2010

Training Center

was opened

16 Advanced training courses for information security professionals

2 Cybersecurity courses for users

PRODUCTS AND SERVICES

SearchInform FileAuditor

The amount of data a regular company stores is enormous, and some of it contains confidential information such as personal and financial data, blueprints, and more. Each category of sensitive data must be stored, processed, and shared in accordance with relevant regulations.

- CRITICAL DATA ALWAYS AT FINGERTIPS
- FILE PROTECTION IN ANY APPLICATION

SearchInform platform provides a comprehensive MULTILEVEL PROTECTION against information security threats.

LEVELS OF INFORMATION SECURITY covered by SearchInform products:

FIRST LEVEL	SECOND LEVEL	THIRD LEVEL
File system protection, implemented with the help of FileAuditor (DCAP tool).	DLP system ensures protection at the level of workstations, data channels, and human-related risks.	Risk Monitor provides a comprehensive solution for managing risks and protecting data.

The systems are seamlessly integrated, run on a unified technological platform, and can be deployed within a few hours.

CRITICAL DATA ALWAYS AT YOUR FINGERTIPS

SearchInform FileAuditor is a DCAP (Data-Centric Audit and Protection) solution designed for the automated auditing of information storage systems. It identifies access violations and tracks changes made to critical data.

Here's how FileAuditor addresses the challenge of monitoring critical data security:

Classification of vulnerable data

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

Access rights audit

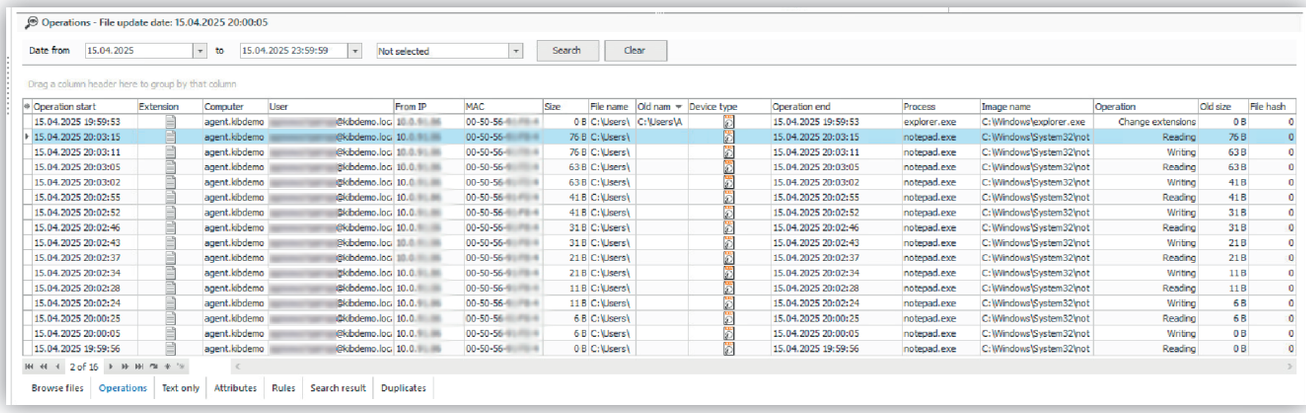
Controls access rights to information (full access, editing, writing, reading, etc.). Tracks employees who have unauthorized access to data. Detects confidential files stored in violation of established security rules (in the public domain, shared network folders, employee PCs, etc.)

Critical documents archiving

Makes shadow copies of important files found on a PC, server, or in network folders and records the history of changes to them. The confidential data archive helps in incident investigations and ensures the recovery of lost information.

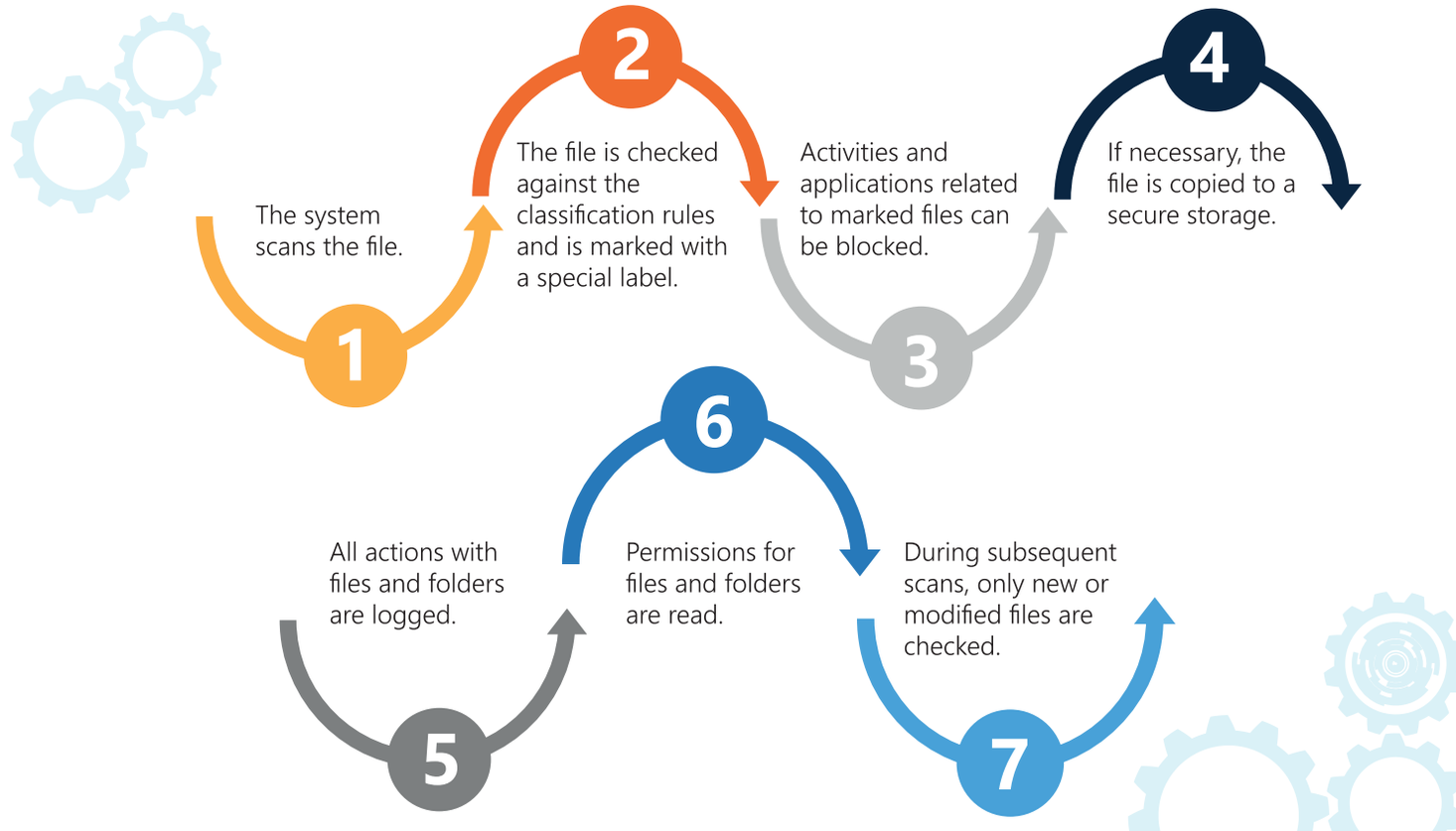
Monitoring and blocking user actions

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



Active Mode: file activity monitoring

HOW SEARCHINFORM FILEAUDITOR WORKS?



The collected information is stored in a database, important documents remain accessible even after they are deleted on users' computers.

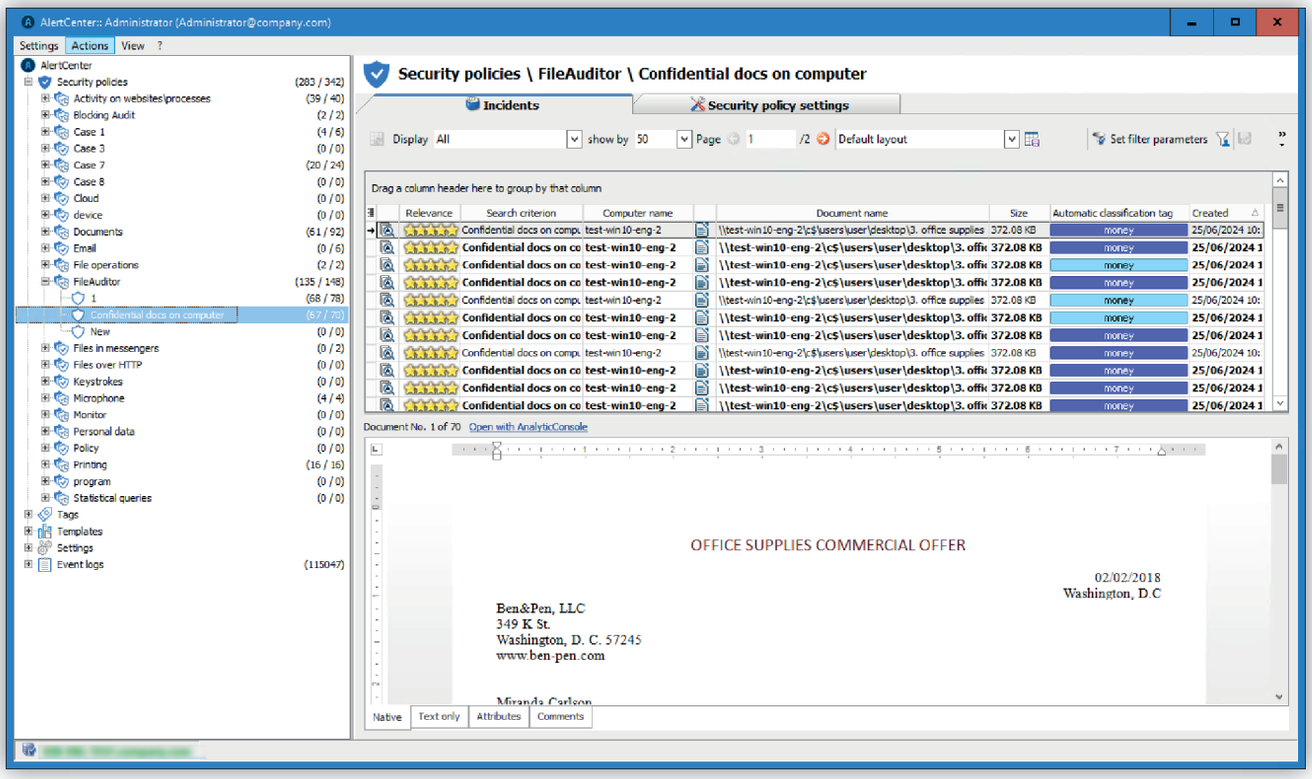
DATA ANALYSIS

FileAuditor's analytical module visualizes the results of file system scans according to predefined rules. Rule settings support various search types. The results can be displayed as visual reports (e.g., sources, access rights, errors) or in a tree format.

The program demonstrates:

- A folder tree indicating user rights for each directory or file;
- Operations on critical files, including creation and modification dates;
- The number of critical documents on a disk or in a folder;
- File labels, for example, NDAs, personal data, financial statements.

Policy violation notifications can be configured in AlertCenter. For instance, if FileAuditor identifies a sensitive file on a user's computer without the appropriate access rights, the designated risk mitigation officer will be notified automatically via email.



AlertCenter

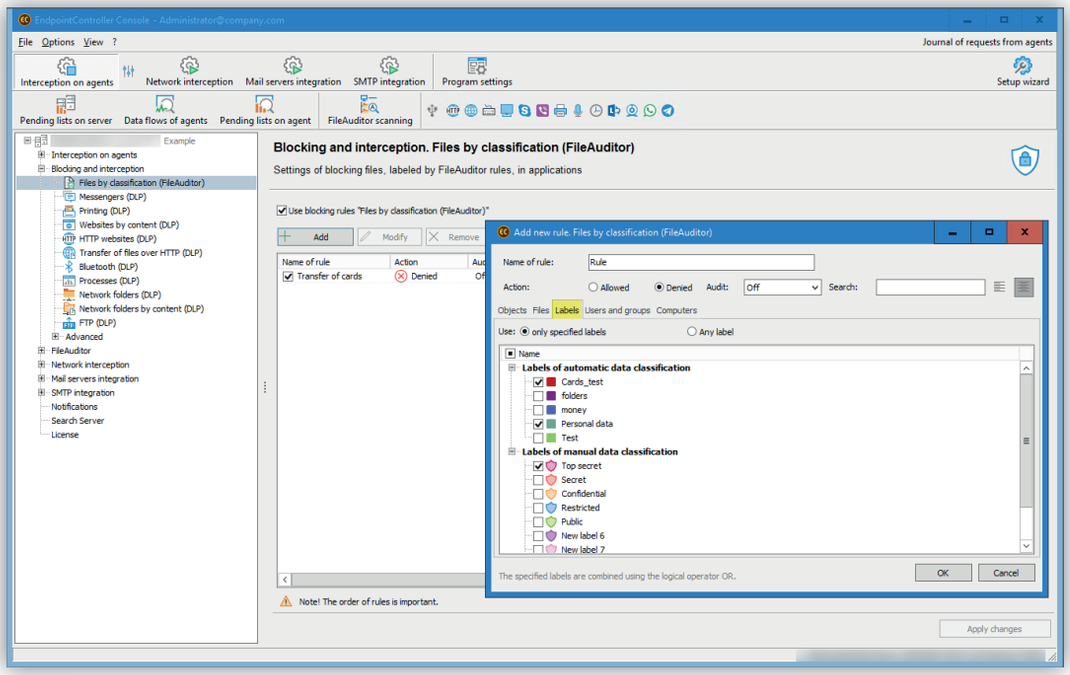
Information collected by agents and the network scan module is stored in a database running Microsoft SQL Server or PostgreSQL, while copies of critical files are maintained in the repository. This ensures that documents remain accessible even after deletion.

DATA PROTECTION

Content-based blocking prevents critical file operations, including unsanctioned actions with documents across various applications, suspicious transfers, or access by unauthorized users.

Blocking rules apply to both automatically tagged and manually classified files. The system sets labels based on the type of information — such as trade secret, personal information, or contracts.

Permissions and restrictions are configured according to information classification, defining which users, devices, and applications are allowed to interact with specific file classes.



Setup of blocking rules by labels in SearchInform FileAuditor

FileAuditor allows blocking access to files through any application, regardless of its version, type, or origin. Restrictions are enforced at the file system level, where the system controls whether applications are allowed or denied access to read data. This enables control over the reading, modification, and forwarding of documents containing confidential information, as well as the capability to configure other file access settings.

ADVANTAGES

- Seamless integration of a DCAP solution into the functionality of the DLP system.
- PC load control and memory saving – monitoring can be scheduled or triggered by specific events or conditions; it is possible to retain only sensitive documents, and a deduplication system helps save storage space.
- Cloud deployment capability – the software can be deployed in the cloud, enabling companies without their own IT infrastructure to use the system.
- Flexible rule settings allow specialists to avoid unnecessary tasks and focus only on monitoring critical data.
- Real-time tracking of file changes – the system saves a specified number of file versions, aiding internal investigations.
- Proactive file protection – the system can block access to documents to prevent unauthorized modifications or transfers.

SearchInform DLP

Protects the company from confidential information leaks and controls data in motion.

Monitors all popular data transfer channels, analyzes content, detects and prevents violations, and provides reports for responsible personnel.

SEARCHINFORM ENSURES RELIABLE PROTECTION OF DATA IN MOTION

Keep your corporate data safe and take advantage of the following features:

- Control over major data transfer channels used for business operations;
- Unique analytical tools, including OCR, similar content search, and Image Search;
- Detailed incident archiving for comprehensive audit and investigation;
- Deployment options include on-premises installation or cloud deployment, with support for integration with Microsoft 365.

1. Monitors the most commonly used data transfer channels in corporate communications.
2. Takes control of remote access and visualization tools.
3. Automatically checks data against preconfigured security policies.
4. Notifies the information security officer and prevents the transmission of confidential data in the event of a potential incident.
5. Alerts on suspicious activity and anomalies within the network.
6. Creates incident archives with detailed records of user actions.

Full compliance with regulatory requirements

The solution helps ensure consistent compliance throughout an organization.

Pervasive data protection and threat prevention

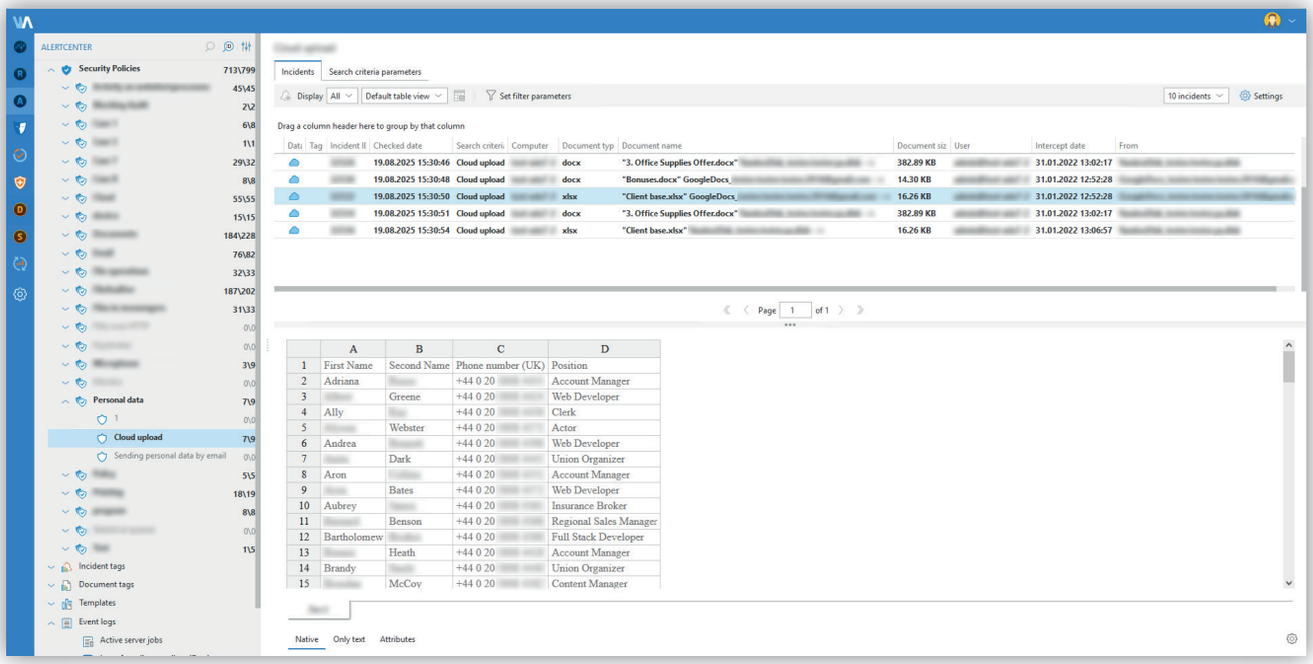
SearchInform DLP identifies and analyzes vulnerabilities in data transmission and leverages advanced analytics to correlate threats.

24/7 protection of your corporate data

The solution safeguards information regardless of where your employees are located.

SECURITY POLICIES

The system offers 250+ preset security policies, both general-purpose and industry-specific. Also, there is a possibility to create custom security policies.



Security policies in AlertCenter

ADVANTAGES

- **The highest quality protection available on the DLP market,** offering content-based prevention of data leaks through messages and files in messaging applications, email, cloud services, remote desktop, web browsing, printing, and removable devices.
- **Support for Windows/Linux/Mac-powered workstations,** DLP server for Windows and Linux, MS SQL Server and PostgreSQL databases, optimized for storage and analysis.
- **The most advanced analytical technologies on the market,** featuring classical patterns (over 430 provided by default), intelligent algorithms, machine learning, and behavioral analytics.
- **The solution is capable not only of implementing blocking,** but also of modifying data (encryption, quarantine, mail return to user).
- **DLP provides access to unique technologies** automated profiling, which enables the evaluation of human-factor risks and even supports appropriate management decisions.

SearchInform Risk Monitor

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

Risk Monitor protects your business from financial and reputational losses caused by internal threats.

SEARCHINFORM SOLUTION ON-PREMISES AND 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: Risk Monitor collects, processes, and stores data in a virtual environment. This deployment model is suitable for companies that don't have their own IT infrastructure, have offices in different cities, and a large number of employees working remotely.

SINGLE-AGENT COMPREHENSIVE RISK MANAGEMENT PLATFORM

User-Centric Security

- Helps to increase staff productivity
- Safeguards the company against personnel risks and predicts employee behavior patterns
- Assists with team loyalty management
- Controls the human factor

Facilitating Compliance

- Solves regulatory compliance issues
- Conducts forensics and retrospective investigation

Data-Centric Security

- Mitigates the risks of data leaks
- Protects for the most sensitive data on corporate devices

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, detecting potential threats or preconditions for violations and alerting to possible risks

Risk Monitor provides you with a powerful and automated toolset for monitoring employees, assessing risks, and conducting internal audits. It ensures that your company's policies comply with relevant regulations and helps you evaluate the alignment of your security measures with the latest industry standards.

The solution is based on a risk management framework, which exposes corporate fraud and prevents financial losses.

CAPABILITIES

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 enhances security policies to minimize risks

Helps increase staff productivity and supports team loyalty management

Alerts to a potential threat before an incident occurs, thereby promoting a corporate security culture and boosting internal threat awareness

DATA COLLECTION CAPTURING

The SearchInform solution ensures the protection of all commonly used data channels.

E-mail

Email collection, categorization, and quarantine. Protects corporate and public email (Gmail etc.). Protects standard email protocols (IMAP, MAPI, SMTP) and email in browser.

Monitor+Keylogger

Captures screenshots and records the user's screen, including software activity. Takes photos or videos via webcam, logs keyboard input, detects attempts to photograph the monitor, and supports biometric user identification via facial recognition.

IM

Collection, categorization, and blocking of messages, calls, and files transmitted through both corporate and publicly available messaging platforms, including WhatsApp and Telegram.

Connected devices

Collection, categorization, blocking, and forced encryption of files transmitted via input/output ports on data storage devices.

Software

Tracks time spent in applications and browsers, evaluates productivity, and analyzes user activity during corporate investigations.

Cloud services

Collection, categorization, and blocking of files transmitted to cloud services or collaborative software (for example, Zoom).

Microphone

Automatically transcribed audio is analyzed by the system to identify potential violations of security policies.

HTTP

Collection, categorization, and blocking of any browser traffic not captured by other controllers.

FTP

Collection, categorization, and blocking of FTPs traffic.

Print

Collection, categorization, and blocking of files sent for printing.

CONTROL CENTER

DataCenter

Manages product indexes and databases, monitors system health and ensures connectivity to third-party systems, like Active Directory, SOC, and the outgoing mail server. User access rights are managed from DataCenter.

AlertCenter

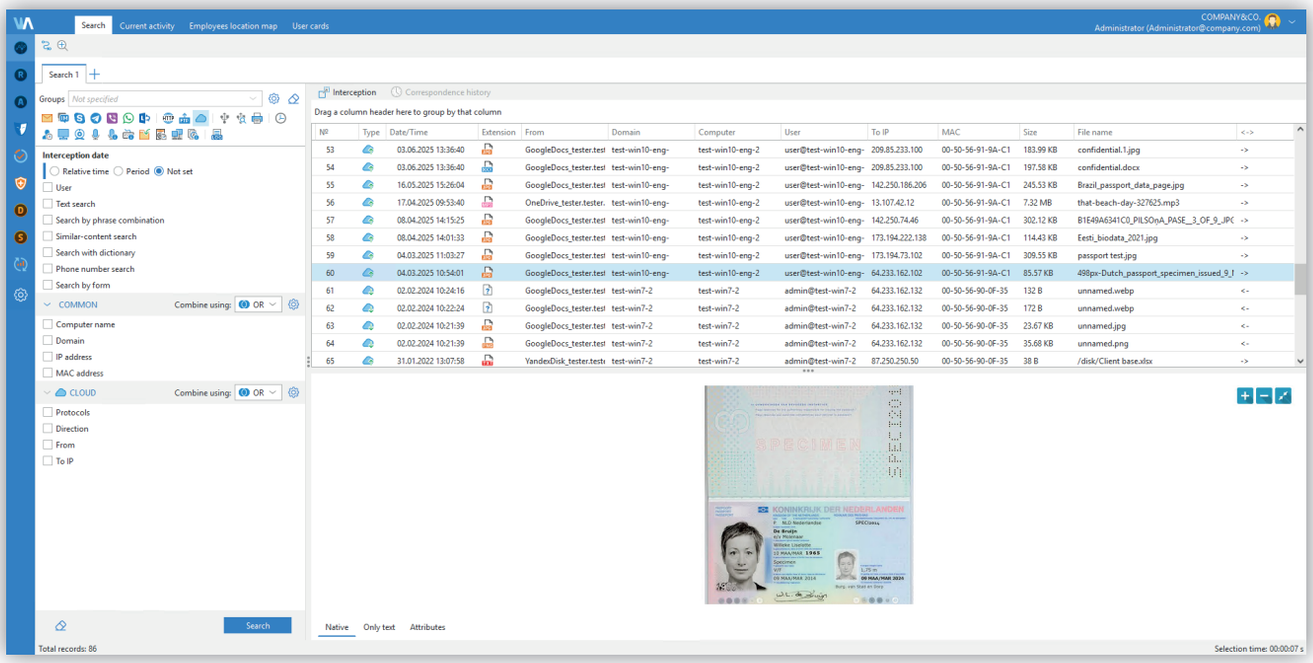
This is the system's "think tank" where security policies are set up. It includes 250+ preconfigured security policies that can be edited. The solution makes it possible to create custom policies for captured data check and blocking, configure the schedule of checks and send notifications.

Security specialists can view incident reports in the AlertCenter console on their workstation or via the web interface accessible from a laptop, tablet, or smartphone.

AnalyticConsole

The AnalyticConsole is used to analyze intercepted data and monitor user activities. It provides various search algorithms and preset report templates for experts to use.

All the features of AlertCenter and AnalyticConsole are accessible through a web interface. In such a way, security specialists can quickly react to alerts and take immediate action against potential threats.



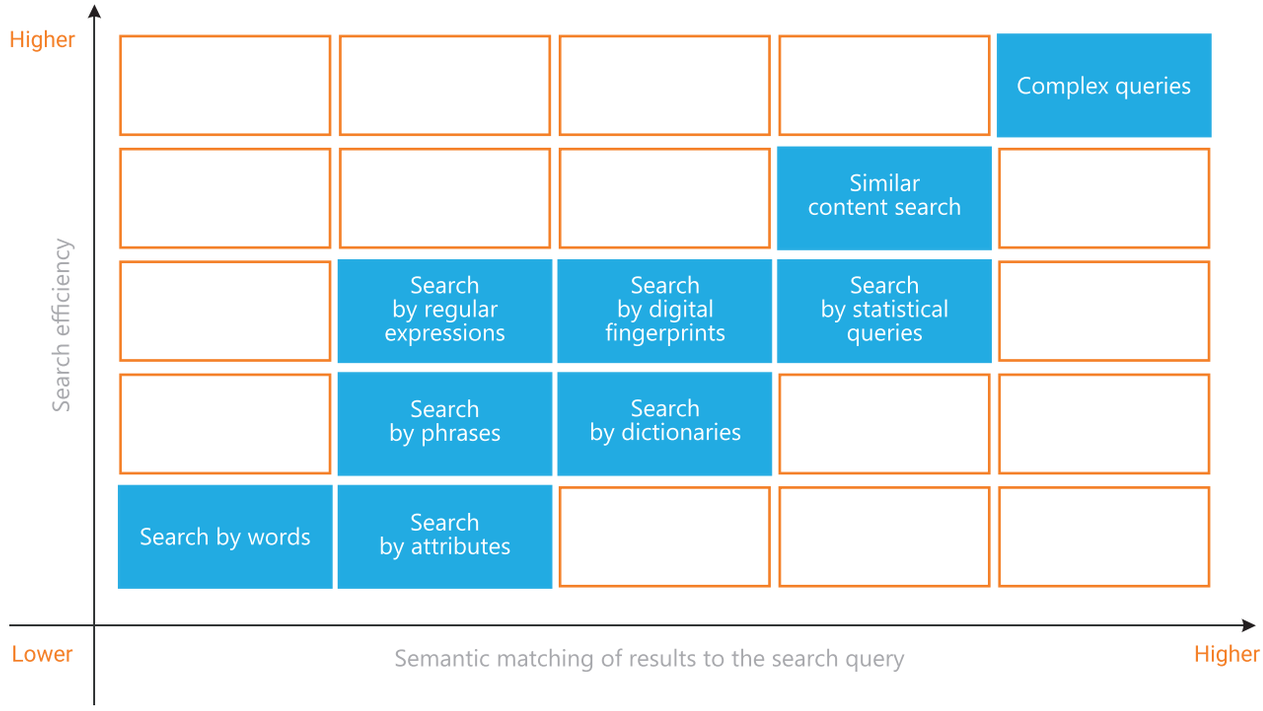
Search Module in the SearchInform Risk Monitor web console

ANALYTICAL CAPABILITIES

To boost their performance, security specialists need comprehensive control capabilities across all communication channels, as well as sophisticated functionality to search through and analyze captured data. 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

Unique search technologies, such as similar content search and complex queries, provide in-depth analysis of text messages and documents. For instance, the similar content search algorithm can identify confidential records even if they have been modified. It searches files that are semantically similar to the query, rather than just technically matching. Complex queries combine several search algorithms, connecting simple queries with logical operators such as AND, OR, and NOT.



Graphical content analysis

The system determines the types of images circulating within the company: PDF files, photos, or scanned copies – and categorizes image files accordingly. The internal classifier identifies documents that conform to specified patterns: passports, bank cards, driving licenses, etc. The technology allows the system to find personal, financial, and any other sensitive data in the archive, even when transmitted in the form of scanned documents.

Audio analysis

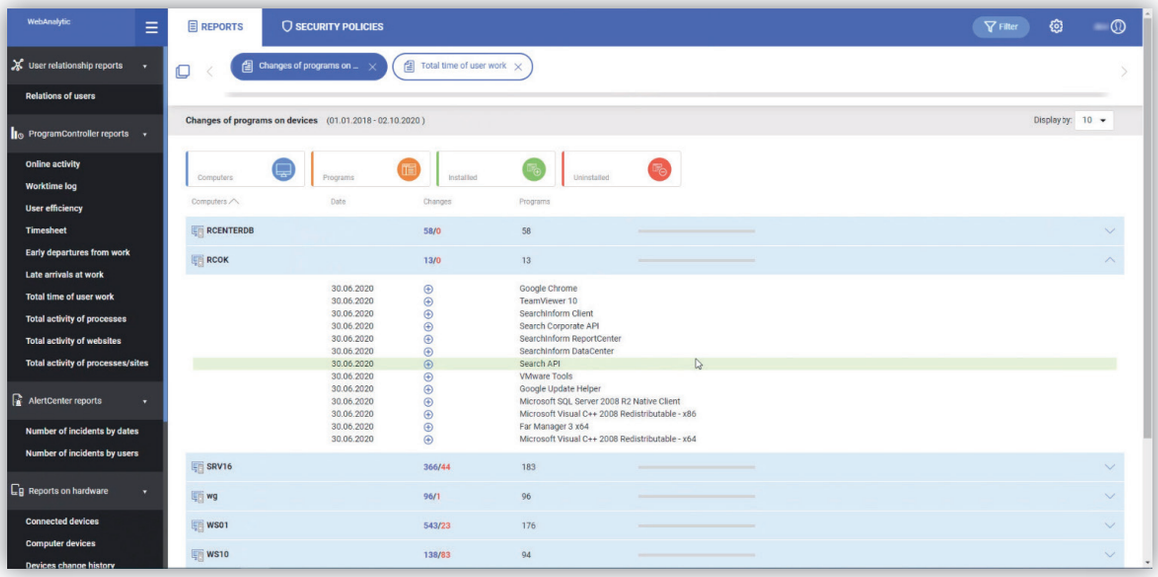
The SearchInform solution converts audio records into text and checks whether a transcript complies with the security policies. The system has an option to turn on audio recording when speech is detected or when certain processes or programs, as specified in the settings, are started.

REPORTS & UEBA

Risk Monitor visualizes all events and connections within a company in the form of reports, available via the AnalyticConsole and the web interface. By default, the system offers more than 30 standart report templates. The report wizard allows you to create custom reports with no limitations on criteria.

Software and hardware report

The solution reports any changes to the installed hardware and connected devices, helping with inventory management and preventing equipment theft or unauthorized replacement. Risk Monitor also reports on software installations and uninstallations.

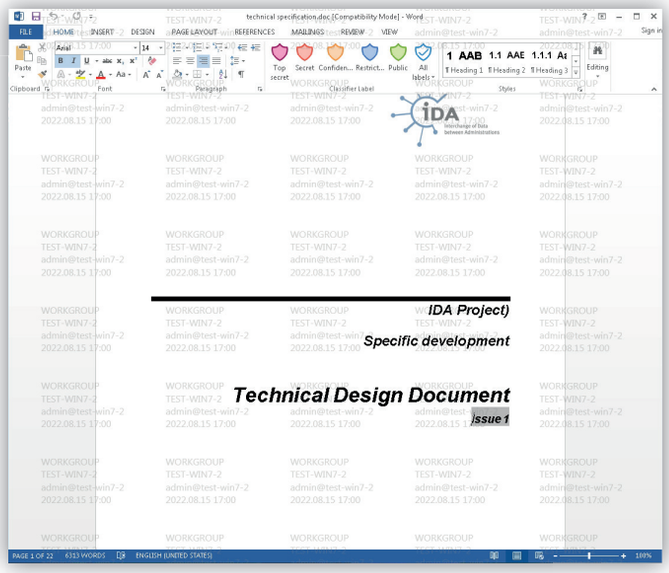


Software and hardware report

INVESTIGATIONS AND CONTROL

Leak detection when data is exfiltrated through screenshots or screen photos

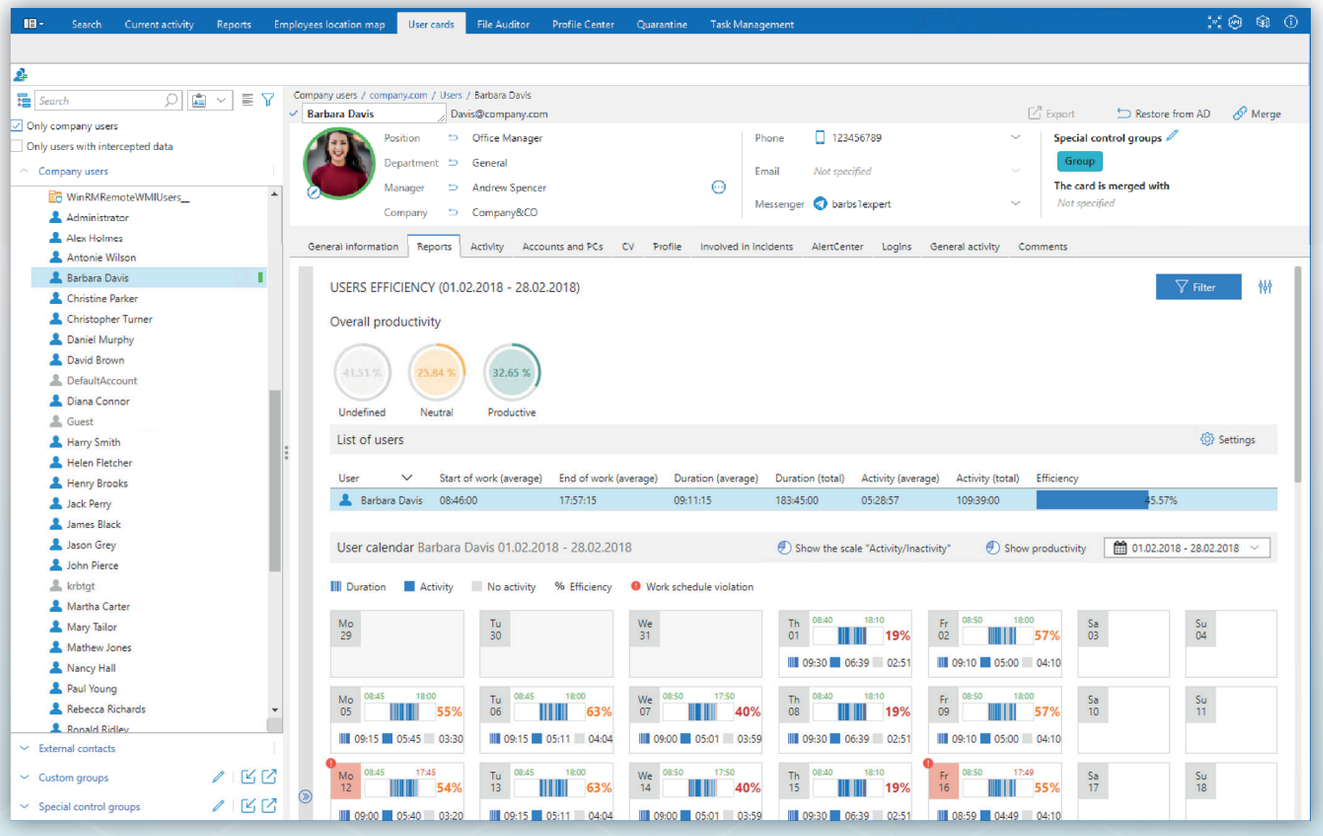
Detecting the source of the leak when a user is taking screenshots or screen photos is extremely hard. The SearchInform Risk Monitor watermarking tool deals with the task. By analyzing a screenshot or a photo of a screen from a protected workstation found in an external source, an information security professional can easily identify the origin of data leakage using displayed watermarks. The watermark contains an indication of the PC and the employee who works on it.



Watermarks layered by Searchinform Risk Monitor

User cards

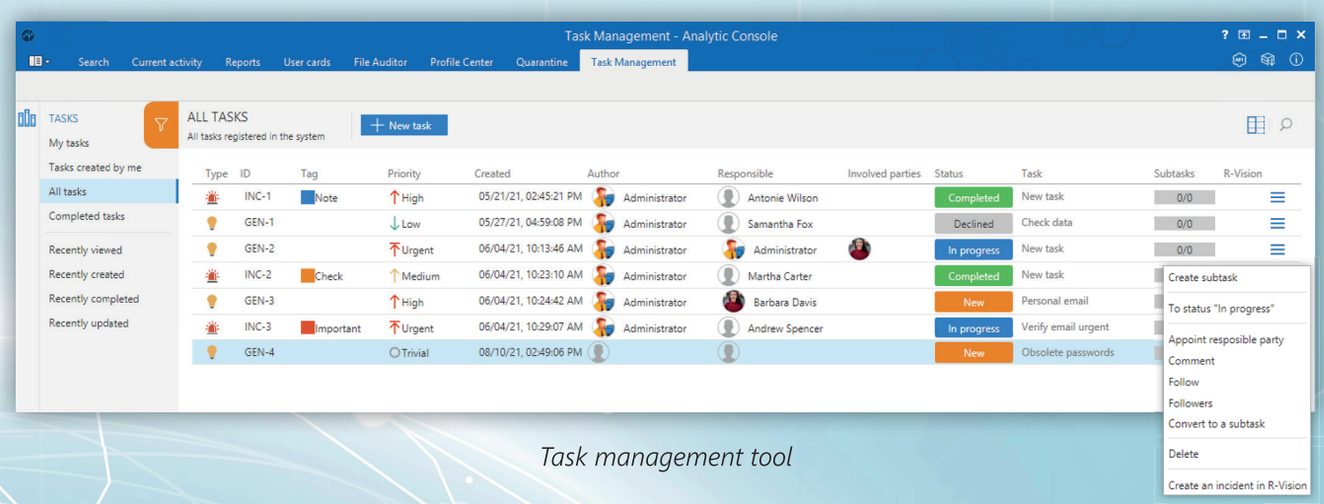
The User Card collects a "dossier" on each employee, automatically including all the incidents in which they are involved. User Card contains individual reports, personal details of the employee, their job history, and other information.



User cards

Investigation Management

Task Manager helps security specialists coordinate information security tasks. It allows them to distribute tasks, track the progress of investigations, and generate reports on the results, including transferring them to the SOC.



Task management tool

UNIQUE FEATURES

1

Unique analytical features unavailable in any other tool

Risk Monitor has a range of analytical features, including common tools such as dictionary searches, regular expressions, and digital fingerprints. It also provides advanced features such as search for similar images, accessing audio records using speech-to-text technology, and analyzing content in video recordings of user activity.

2

High-quality investigation tools in one solution

Risk Monitor records audio of employees' speech and video of their actions. The solution logs all types of users' operations with files and folders and audits logs, devices, and software. It also monitors violators through audio and video channels in real-time.

3

Control of users' efficiency

SearchInform Risk Monitor automatically evaluates a users' efficiency in various applications and on websites. This function helps to strengthen discipline in a company and detect problems within business processes.

4

Confirmed system stability under load

SearchInform is trusted by large-scale enterprises across various industries, demonstrating the system's stability under high load and in diverse IT environments.

5

Feature extension through a unified product ecosystem

SearchInform offers a comprehensive suite of products, including Risk Monitor, DLP, SIEM, and FileAuditor (a DCAP solution). All systems are built on a unified technological platform, enabling seamless integration and deployment within just a few hours.

6

Cross-platform and accessible from any device

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

ADVANTAGES

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.

Proactive incident protection

Risk Monitor provides smart content blocking for all controlled channels to ensure users will not be able to transfer files and messages with confidential content. The interface on agent notifies users of accidental policy violations, promoting a culture of information security.

Remote access control

The SearchInform solution protects data transmitted through virtual environments and remote access tools. Monitoring is implemented both at the clipboard level, during virtual storage device connections, 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 4,000+ companies operating in multiple sectors 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 the SearchInform solution within a few hours. The installation process does not hamper the operation of the company's local information systems.

Incident investigation tools

Online activity control tools such as recording conversations, capturing on-screen content in real-time, monitoring keyboard inputs, making videos with a webcam, and creating information flows and connection graphs can help reconstruct security incidents step by step. The Task Manager and automated incident search tools enhance the performance of information security teams.

Elements of AI

The system automatically identifies users' faces and determines whether a PC is being operated by the owner. Risk Monitor detects attempts to take pictures of a computer screen with a smartphone and leaves digital traces by applying unique watermarks to help identify the origin of a potential data breach.

Cloud deployment model

All the components of Risk Monitor can be deployed in the cloud (the SearchInform cloud or any third-party cloud service can be used) without interfering with the system's functionality. This is a cost-effective and time-efficient method of deployment.

Integration with other SearchInform products

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

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, come late to work or leave early.

TEAM ACTIVITY

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

TimeInformer scans corporate PCs and helps you identify:

- Violators of workplace discipline who come late, leave early, take frequent smoke and coffee breaks
- Freelancers who do side work during the hours paid by the company
- Idlers who chat, shop online, get distracted by games and other activities
- Unsatisfied employees who turn other workers against the employer, or who have become exhausted because of heavy workload or boring tasks

TimeInformer monitors the idle and working times of employees and collects data on the software they use during the day. It records all the websites they visit and categorizes them into different groups, such as dating sites, online shopping, news, and TV shows, and others. This information is then used to evaluate the actual productivity of the staff based on predefined parameters.

REAL-TIME CONTROL

TimeInformer can operate not only in the background but also in several active modes. The program connects to PC monitors and microphones, allowing you to observe real-time activity on employee workstations.

It records important negotiations with key partners and clients, capturing both audio and screen activity in real time. The solution also enables live monitoring of up to 16 employee screens simultaneously.

TimeInformer monitors corporate PCs and helps you identify: need to purchase or maintain additional hardware.

ASSISTANCE IN MANAGEMENT DECISIONS

33 pre-set reports in TimeInformer provide a smooth start, allow quick detection of idlers, help to optimize work processes, organize teams, and ensure goals are achieved.

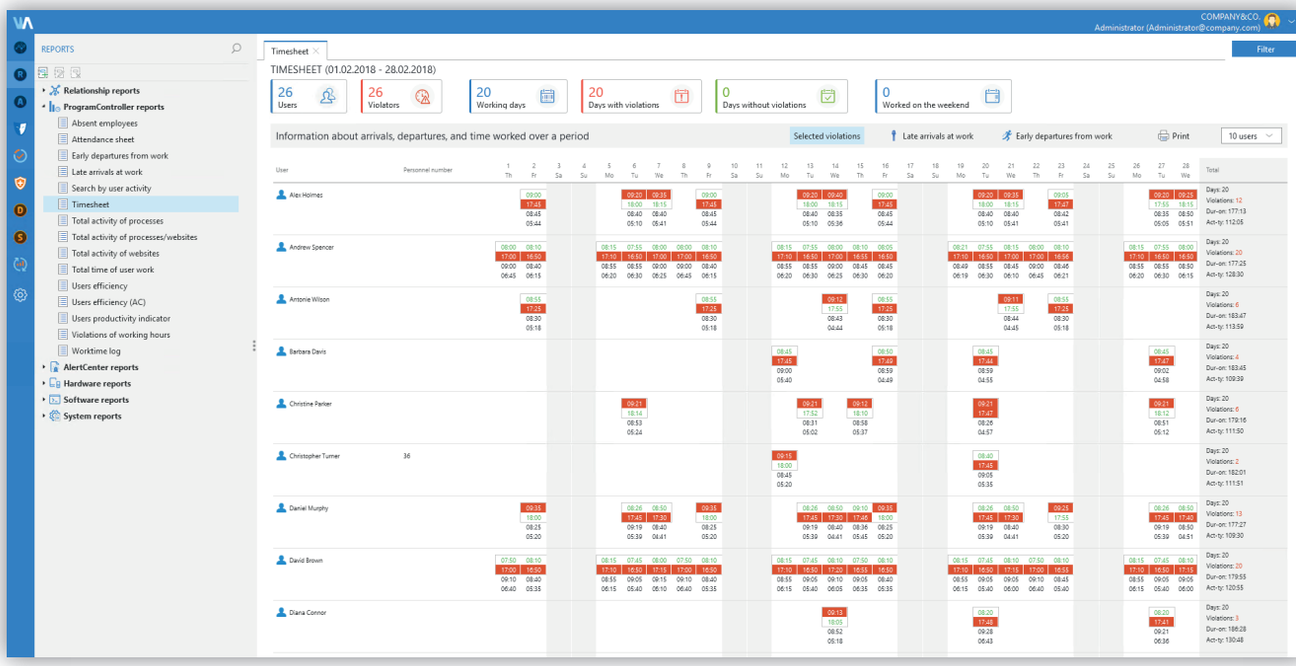
TimeInformer offers the following groups of reports:

- Reports on user activity in applications and on websites
- Reports on programs, including the history of software installation and removal
- Reports on devices, with data on equipment installed on a PC and changes to their configuration

Reports and notifications can be easily customized. The system automatically notifies administrators of policy violations.

USER-FRIENDLY INTERFACE

The web interface allows managers to oversee employees from anywhere in the world. Access to reports and administrative functions is customized based on roles and responsibilities. Automatic email alerts notify administrators of any suspicious employee activity.



Timesheet in the web interface

ADVANTAGES

- Protected from deletion and configured to alert on any deletion attempts
- User activity monitoring, even when they work from home or are on business trips
- Web interface to access monitoring results outside the office
- Integration with SearchInform products, which helps perform internal investigations

SearchInform Managed Security Services

MSS by SearchInform ensures continuous protection of sensitive data and helps improve business efficiency.

WITHIN THE SERVICE THE CUSTOMER GETS:

- Data leak prevention
- Monitoring employee productivity and detecting patterns of systematic idleness
- Corporate fraud detection (kickbacks, moonlighting)
- Know-how and intellectual property protection
- Mitigating the risk of losing key talent
- Security incident investigation

HOW IT WORKS?

30-DAY FULL-FEATURED FREE TRIAL

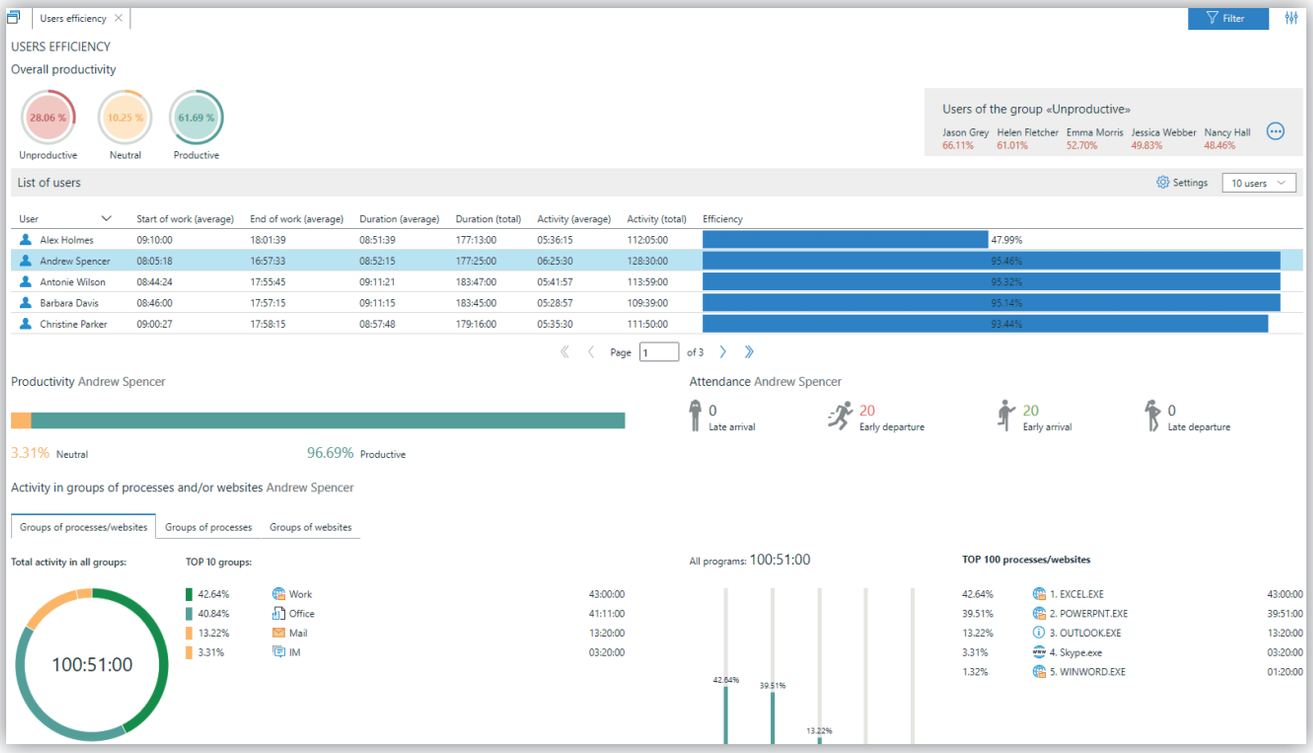
During the free trial, you'll perform an audit of your organization, identify data protection issues, obtain practical results, receive expert advice on enhancing corporate security, and evaluate whether MSS meets your requirements.

TASK – SOLUTION

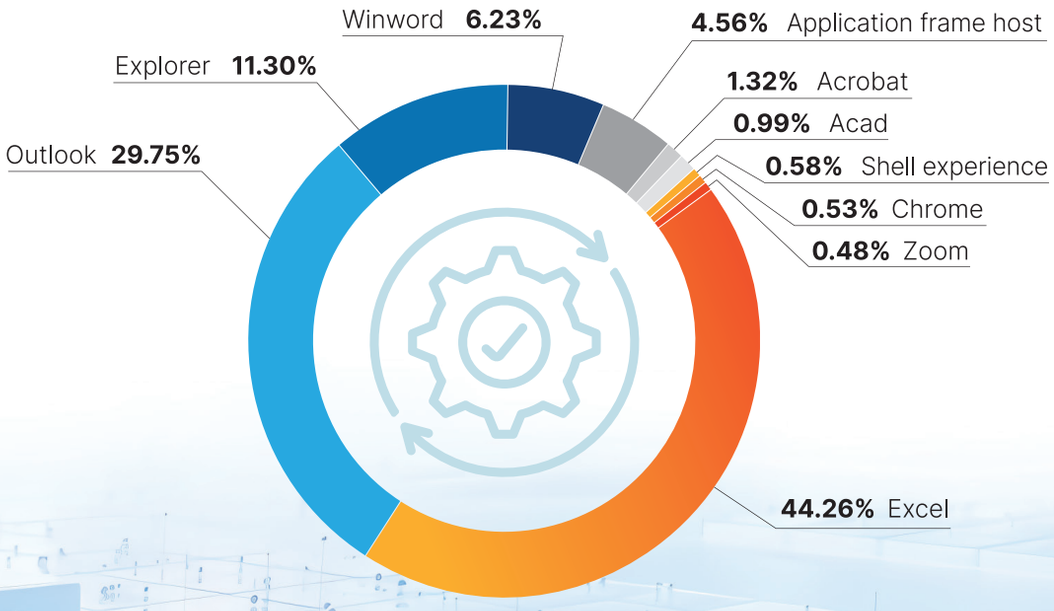
Clients gain full visibility of actual organizational activities through comprehensive, data-driven reports.

Date	Employees involved	Comments	Link to documents
External Devices			
05/06/2024	John Smith	An employee connected personal USB flash drive to the corporate computer and attempted to copy large amount of data. The process was blocked, and data leakage was prevented. The investigation revealed that the employee had tried to copy customer database and sell it later to a competitor.	full factual Info
Data Leakages			
21/06/2024	Ömer Aydın	Analysis of correspondance in corporate WhatsApp revealed a data leak incident. The employee discussed an oncoming deal with representative of the market competitor, they communicated via IM. Lately the employee has shared a few commercial documents related to the deal with the competitor via WhatsApp.	full factual Info
01/07/2024	Barabara Davis	Employee intended to breach data: he created an email draft in personal Google mailbox using corporate laptop and attached confidential financial data and files (incl. phone bill). This would enable the insider to access the data outside of the corporate perimeter after some time without even sending the email.	full factual Info
Document Forgery			
05/07/2024	Danielle Murphy	Procurement department employee forges incoming commercial offers from suppliers with the help of graphic editor. He changes the sums mentioned in the offers.	full factual Info
Side companies			
14/07/2024	Bhupesh Ghoshal	The signs of document forgery were detected. The investigation revealed that the employee used to edit documents of third-party company, which turned out to be the competitor, and the employee was its co-founder.	full factual Info
20/07/2024	Khalid Mustafa	Charter documents of some third-party company were found on the computer of one employee from the finance department. The investigation revealed that the founder of this company is this employee's wife. Evidence that this company is the regular supplier can be found in the link to documents section.	full factual Info
Job Search			
29/07/2024	Jamil Faridi	There was found evidence that one employee is currently actively checking vacancies to apply for a job. The employee was receiving job-related emails at: [redacted]	full factual Info
Misuse of Corporate Resources			
13/08/2024	Hasan Demir	An employee uses corporate laptop to play games. The online games use various types of unwanted cookies and show ads which may damage the company equipment.	full factual Info
Risk Group Employees			
20/08/2024	Elif Kaya	One employee from the sales department spends a few hours a week on gambling websites.	full factual Info
23/08/2024	Jane Doe	Correspondence of one employee revealed she had heavy debts and a few people demanded debt repayment from her. The employee works in the finance department, so the risks must be eliminated.	full factual Info
Sabotage			
02/09/2024	Christopher Turner	A resigning employee attempted to harm the company by deleting some confidential data without the possibility of recovery. The employee's attempt was successfully prevented. View detailed report to find out which data exactly the employee tried to delete.	full factual Info

COMPLETE VISIBILITY OF ALL BUSINESS PROCESSES

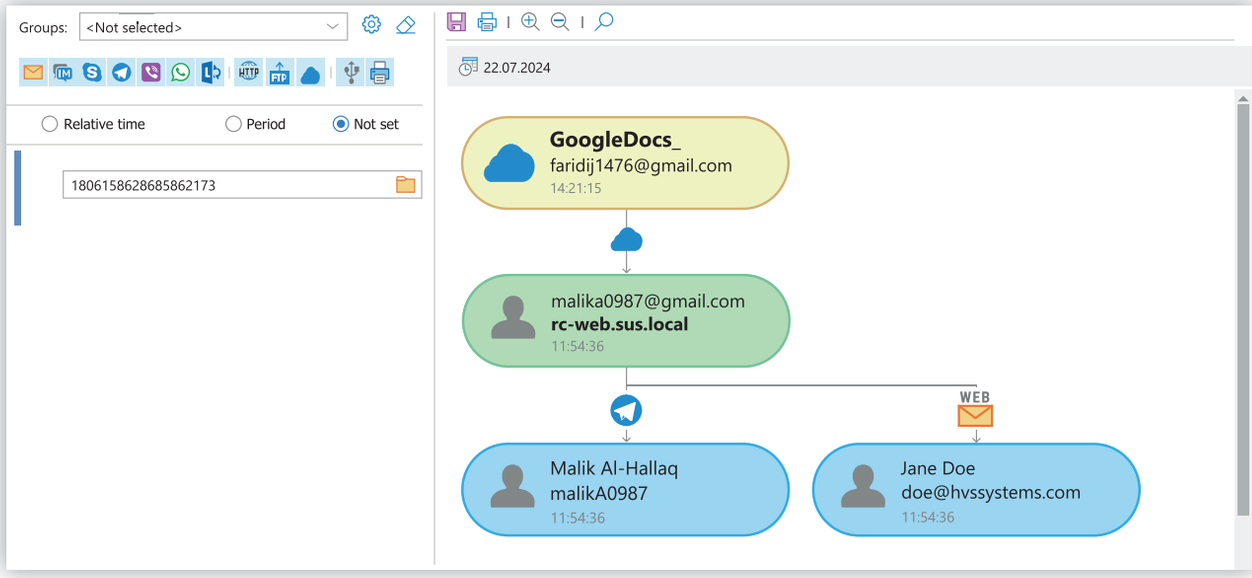


Report on user efficiency



Most used processes

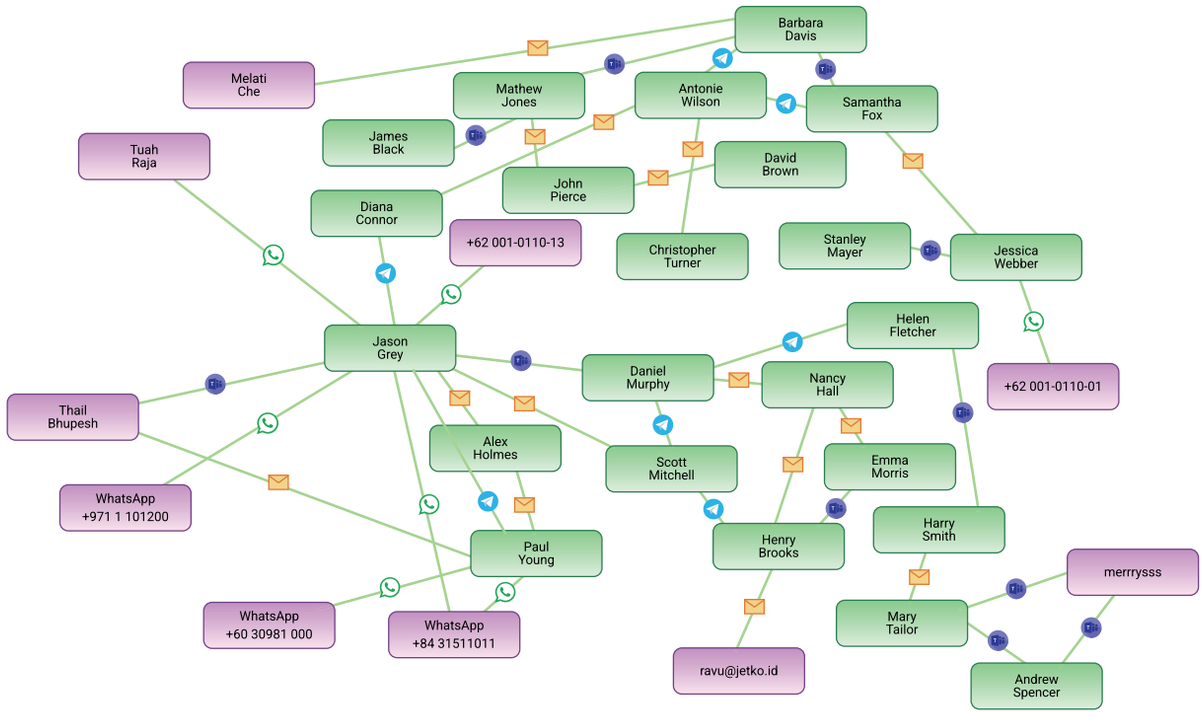
PRECISE ANALYTICS



Content route

A financial report was leaked. The content route report reveals the leaked document's path.

The interconnections report identifies all users involved in the security incident.



User connection report

ADVANTAGES

- **Budget savings** No need to:
  - purchase equipment
  - pay for software licenses and support
  - hire or maintain information security specialists

- **Results without labor costs**

  Delivers advanced protection without requiring in-house experts, overcoming the challenge of finding qualified personnel in the market.

- **Instant effectiveness**

  Identifies vulnerabilities quickly (initial results typically appear within the 1-month free trial period).

- **Unbiased professionalism**

  Our analyst team has no personal relationships with your staff, eliminating human bias during investigations.

- **Vast expertise**

  Analysts leverage a knowledge base built from 4,000+ client cases, configuring protection tailored to your industry.

Microsoft 365 Integration

SearchInform solutions are fully and seamlessly integrated with Microsoft 365

The trend of migrating to cloud services is growing. As applications and data move to the cloud, with information and functionality becoming accessible through browser-based versions, and traditional endpoint protection is no longer sufficient.

Microsoft 365 is one of the most popular cloud services. SearchInform has developed specialized Microsoft 365 protection to safeguard corporate data for its clients.

- The integration is implemented via the Graph API, providing clients with full access to all critical security solution functionalities.
- SearchInform solutions provide protection across all Microsoft 365 services, including: Word, Excel, PowerPoint, Outlook, Teams, SharePoint, OneDrive, etc.

HOW IT WORKS?

Through seamless integration, files and information transferred to Microsoft 365 services (including Outlook) are analyzed and protected by SearchInform FileAuditor and SearchInform DLP directly on the server.

Key protection mechanisms for Microsoft 365 include:

- An agentless protection model for effective safeguarding within a blurred corporate perimeter;
- Use of content-based analytics to accurately determine the content of documents;
- Analysis of the classification labels assigned through Microsoft Information Protection;
- A unified protection environment for cloud, Windows, macOS, and Linux;
- Support for scanning files in SharePoint.

FILEAUDITOR INTEGRATION WITH MICROSOFT 365

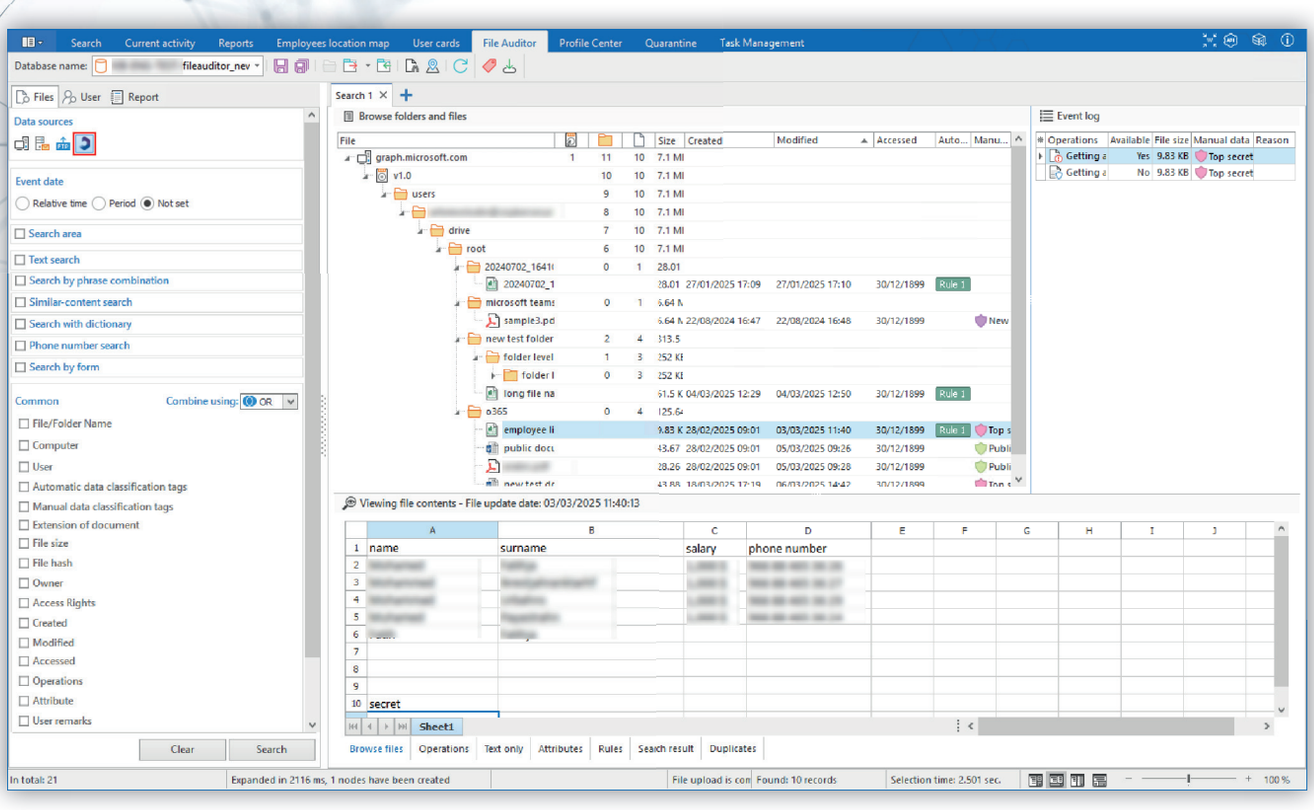
When working with Microsoft 365, FileAuditor monitors all user activity within the corporate perimeter.

The system accesses all workspaces in Microsoft 365 that users interact with.

The solution scans these workspaces and classifies stored files using content-based analytics.

At the same time, FileAuditor automatically organizes files into categories. For example, when a file appears in a Teams chat, the solution creates a dedicated “Microsoft Teams Chat Files” section for storage. This automation reduces routine workload for Information security analyst and improves overall security efficiency.

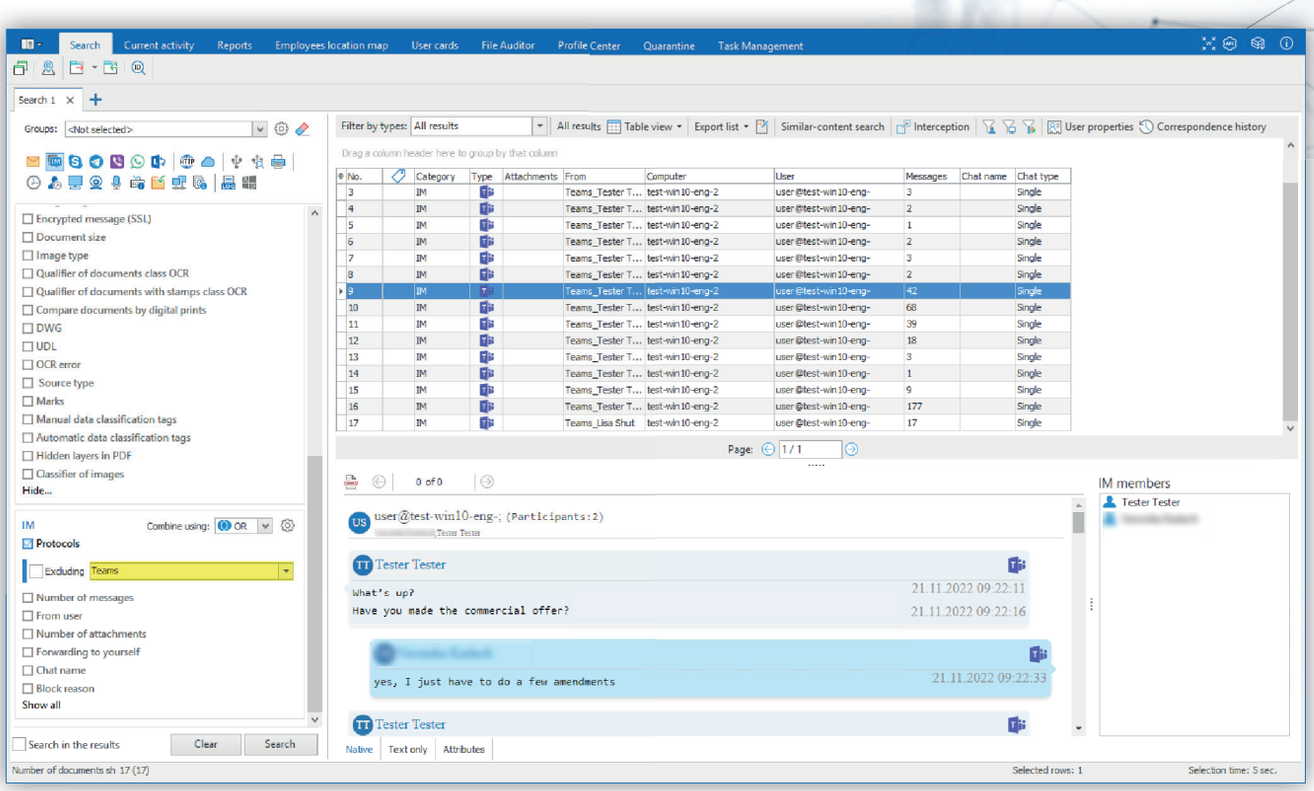
FileAuditor analyzes all files and assigns sensitivity labels based on document content, information type, and sensitivity level. This enables accurate criticality assessment and the enforcement of appropriate security policies.



Result of scanning Microsoft 365 with FileAuditor

DLP INTEGRATION WITH MICROSOFT 365

SearchInform DLP integration with Microsoft 365 provides users with full access to all standard DLP functionalities.



1 The solution controls data transmission across all Microsoft 365 services.

2 The operational principle involves analyzing the context and content of a file to ascertain its type, confidentiality level, and whether it is subject to specific security policies (integration with FileAuditor enhances accuracy and reduces DLP operational costs).

3 All traditional advanced analytics and e-forensics capabilities remain accessible. The Information security analyst receives comprehensive event details, including the original message, transferred files (in their original format), recipient and sender information.

SearchInform SIEM

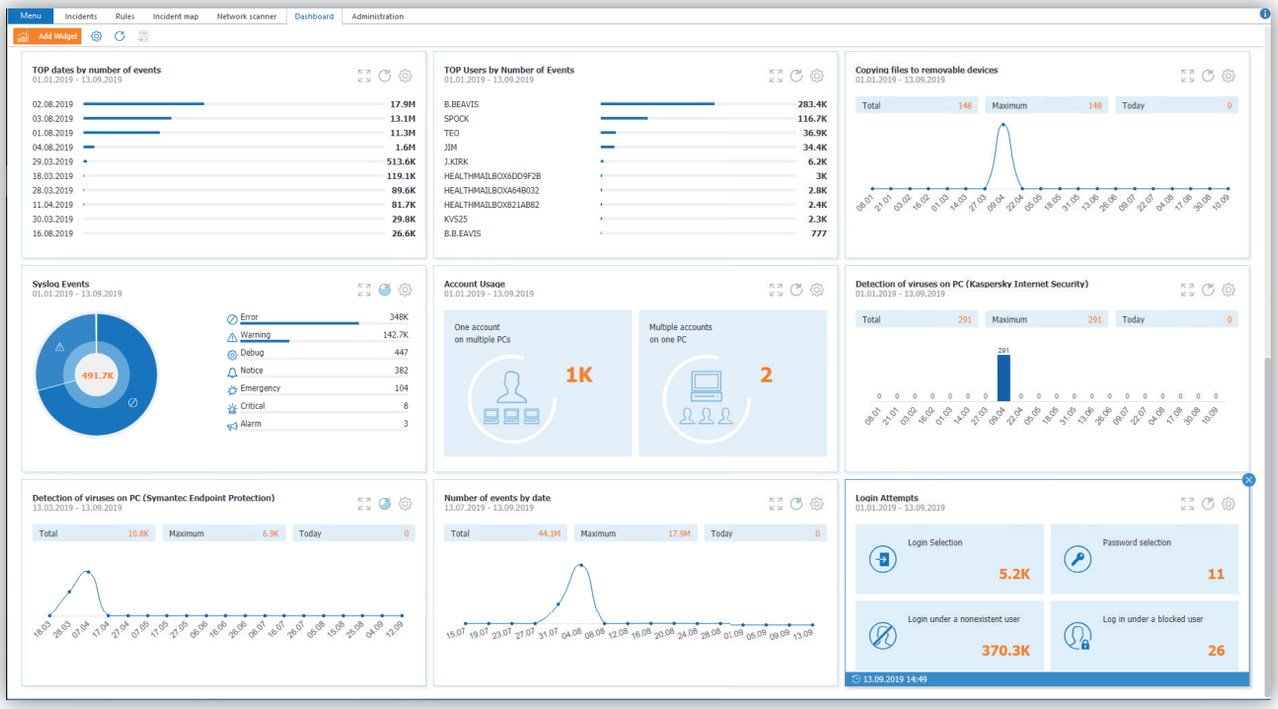
- OUT-OF-THE-BOX SIEM
- CORRELATION RULES CREATED IN JUST 2 CLICKS

Modern enterprise IT infrastructures consist of multiple critical systems: firewalls, operating systems, email servers, databases, and network devices.

These systems represent prime targets for malicious actors, requiring specialized security measures.

Automatic security event monitoring

SearchInform SIEM is a comprehensive solution for real-time security event collection, analysis, and incident response. The system aggregates data from multiple sources, performs advanced analytics, automatically records incidents, and alerts designated personnel.



Event statistics dashboard

SearchInform SIEM identifies:

- Virus outbreaks and individual infections
- Unauthorized access attempts
- Password brute-force attacks
- Active accounts of terminated employees
- Hardware configuration errors
- Permissible operating temperature abuse
- Critical data deletion
- Unauthorized after-hours use of corporate resources
- Deletion of virtual machines and snapshots
- Unauthorized hardware connections to IT infrastructure
- Group Policy modifications
- Unauthorized remote access via TeamViewer or other tools
- Critical security system events
- Information system failures and errors

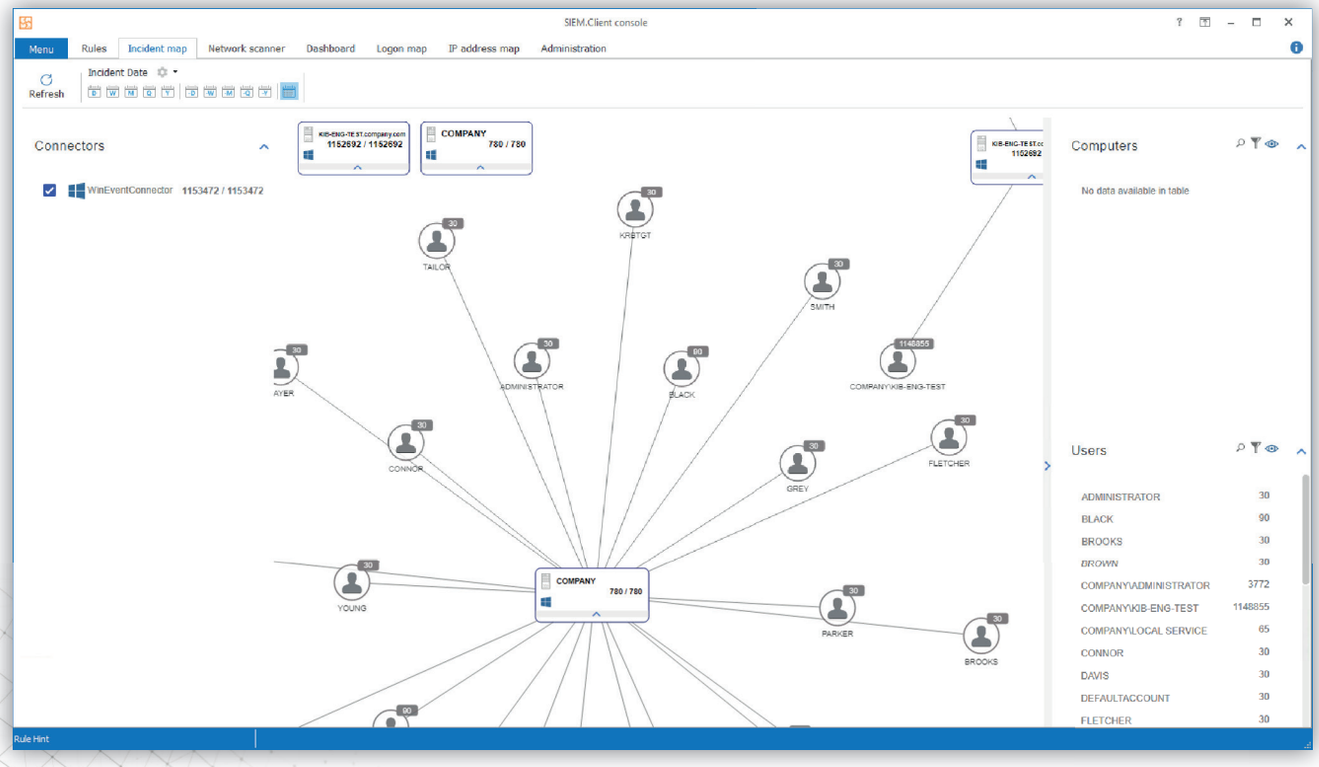
PREDEFINED CORRELATION RULES

Upon installation, the system provides information security teams with 350+ ready-to-use security rules, full customization capabilities, flexible rule creation tools (including user connector customization). Security teams can modify redefined rules and create custom rules, efficiently combining them for better security.

The predefined rules leverage these critical infrastructure components:

- Operating systems
- Email servers
- Domain and workstation controllers
- Linux servers and workstations
- DBMS
- DLP systems
- File servers
- Virtualization environments
- Antiviruses
- Firewalls & network security devices
- All syslog-compatible devices

Cross-correlation rules can be configured to detect complex security incidents by analyzing interconnected events across multiple data sources.



Incident display screen

Predefined correlation rules in SearchInform SIEM:

Mail server monitoring

- Unauthorized mailbox access attempts
- Mailbox ownership changes
- Unauthorized mailbox access permissions granted

Virtualization environment protection

- Suspicious VMware/VWview login/logout patterns
- Repeated invalid password attempts
- Unauthorized snapshot deletions

Domain controller & workstation security

- Temporary account activation/creation
- Single account active on multiple devices simultaneously
- Password brute-force attacks and expired password usage

Resource access control

- Unauthorized access to critical files
- Temporary file/folder permission assignments
- Abnormal multi-user file access patterns

HOW THE SYSTEM WORKS

1. Collects events from various software and hardware sources: network equipment, third-party software, security tools, operating systems.
2. Analyzes 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 security officers when incidents occur.
4. Normalizes and details incidents for further investigation: determines the incident type and source and, when integrated with Active Directory, identifies the user.

ADVANTAGES

- Quick deployment and pre-configuration (operational in one day with instant results).
- Intuitive and user-friendly interface that doesn't require any programming skills to create correlation rules.
- Low hardware requirements, transparent licensing, and cost-effective ownership.
- Preconfigured analytics: includes 350+ ready-made rules leveraging cross-industry experience.
- Incident investigation: examining cases based on single or multiple incidents.

The Risk Monitor integration strengthens information security by supporting end-to-end incident investigations with complete evidence gathering.

CONTACTS

LATAM

Email: s.bertoni@searchinform.com

NORTH AFRICA

Email: m.sayari@searchinform.com

SOUTH-EAST ASIA

Email: order@searchinform.com

RUSSIA

Email: info@searchinform.ru

KAZAKHSTAN

Email: e.matushenok@searchinform.ru

UAE

Email: uae@searchinform.com

TURKEY

Email: salesturkiye@searchinform.com

SAUDI ARABIA

Email: ksa@searchinform.com

Try it now and access valuable resources at **searchinform.com**

OUR CLIENTS