

SearchInform Data Loss Prevention

SEARCHINFORM

CONTENTS

SearchInform Data Loss Prevention System	3
Controlling Data Leakage Channels	3
SearchInform NetworkController	4
Work Principle	5
SearchInform EndpointController	6
Work Principle	7
NetworkController and EndpointController: Advantages of Platforms	8
Workstations Indexing Server	9
SearchInform AlertCenter	10
SearchInform DataCenter	12
SearchInform ReportCenter	13
Analytical Capabilities	16
User Identification	17
Revealing Malicious Intentions of Insiders	18
Controlling Laptops	19
Data Flow Control	20
Controlling User Activity	20
Architecture	21
SearchInform MailController	22
SearchInform IMController	23
SearchInform HTTPController	24
SearchInform SkypeControllert	25
SearchInform DeviceController	26
SearchInform FTPController	27
SearchInform PrintController	28
SearchInform MicrophoneController	29
SearchInform MonitorController + Keylogger and CameraController	30
SearchInform FileController	31
SearchInform CloudController	32
SearchInform ProgramController	33
SearchInform DLP Advantages	33
Contact Details	35

SEARCHINFORM DATA LOSS PREVENTION SYSTEM

Controlling Data Leakage Channels

Today, information is one of the critical assets for success and prosperity of your business. On average, a data leak costs around 5,3 M USD to the information owner.

What are the major data leak channels? There are several data transfer links: email, social networks (Facebook, Twitter, etc.), Internet message boards, web blogs, instant messengers (ICQ, MSN, Jabber, etc.), removable media, mobile devices, printers, FTP servers, and Skype.

If you do not control the above-mentioned channels or control only one or two data transmission links, your company's sensitive information may be easily transmitted to rival companies.

State-of-the-art information security system should allow all data communication channels, and at the same time intercept and analyse data flows transmitted over these channels. Integrated approach to information security is impossible even if only one potential data leak channel is not controlled.

SearchInform Data Loss Prevention (SearchInform DLP) is a recognized leader in the DLP market in Russia and the CIS. The product is used in many large companies working in almost any sector – from banking to engineering.

This software solution provides for efficient control of data links at all levels – from every single user's workstation to LAN servers. All information transmitted over the Internet is also controlled.

SearchInform DLP has a multi-component architecture, i.e. a customer can select only the modules he actually needs. There are two major system platforms: NetworkController and EndpointController. NetworkController intercepts data on a protocol level using a traffic-mirroring device. SearchInform EndpointController uses agents installed on user workstations.

SEARCHINFORM NETWORKCONTROLLER

SearchInform NetworkController is a traffic mirroring platform, i.e. it processes data not interfering with the existing network processes.

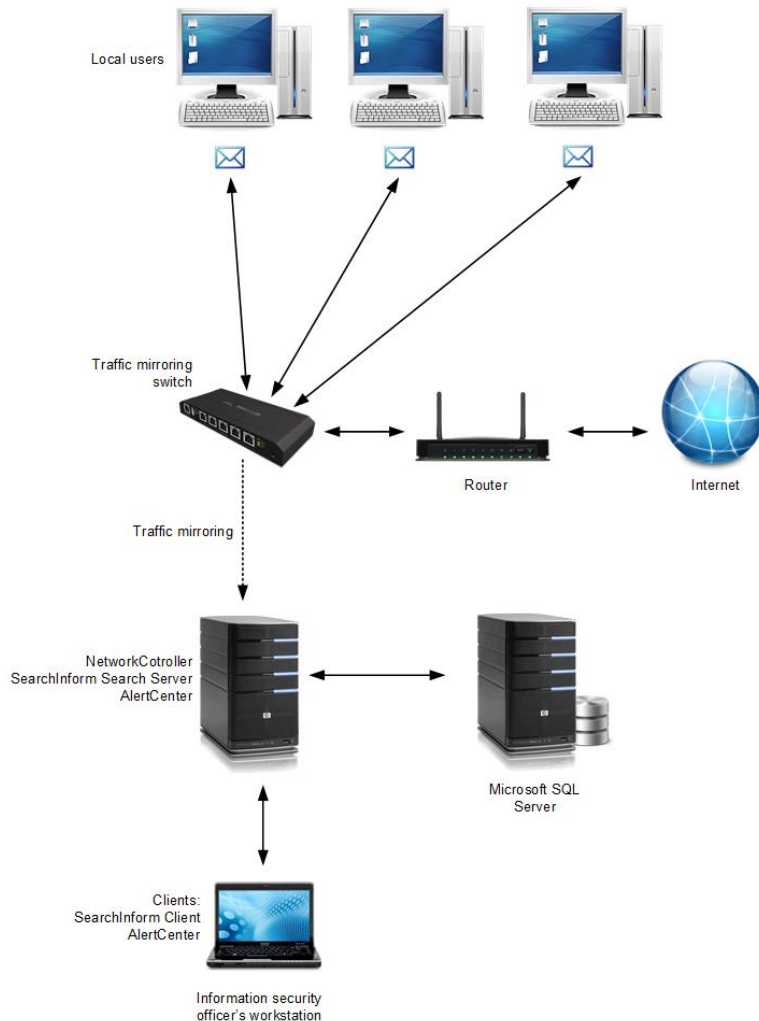
It supports the following protocols SMTP, POP3, HTTP(S), IMAP, MAPI, NNTP, ICQ, XMPP, MMP, MSN, SIP, Gadu-Gadu, and FTP on the level of Local Area Network.

Also, NetworkController includes:

- Module of integration with mail servers that allows extracting messages directly from corporate mail server
- Module of SMTP integration that allows getting containers of log reports.

This platform incorporates the following:

- **SearchInform MailController**
- **SearchInform IMController**
- **SearchInform HTTPController**
- **SearchInform FTPController**
- **SearchInform CloudController**



Work Principle

Traffic is captured on the level of network protocols (Mail, HTTP, IM, FTP, and Cloud). Information can be filtered by domain names, computer names, IP and MAC addresses.

All intercepted messages are stored in the SQL database which is indexed by Search Server. Indexes allow quick search in the database.

SearchInform AlertCenter checks if new information matches a preset search query. Check schedules and query lists are set up by information security officers. If a match is found, SearchInform AlertCenter will immediately send a notification to the person in charge.

SEARCHINFORM ENDPOINTCONTROLLER

SearchInform EndpointController is a platform that uses agents to intercept traffic. It provides additional control of employees outside company's LAN as they may freely transfer confidential data stored on laptops to third parties.

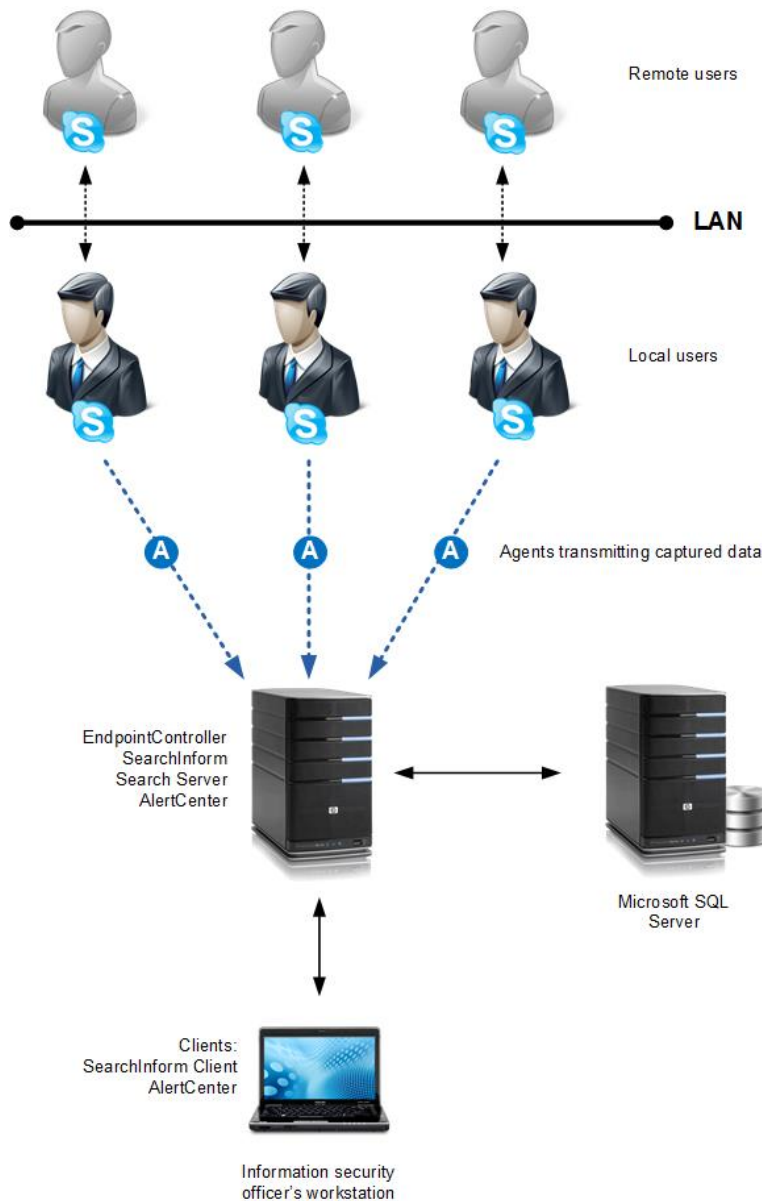
SearchInform EndpointController agents intercept:

- **SearchInform MailController:** all inbound and outbound emails sent through mail clients and web browsers (possibility to block emails)
- **SearchInform IMController:** messages sent over IM clients and social networks
- **SearchInform SkypeController:** voice and text messages, files and SMS sent with Skype
- **SearchInform DeviceController:** data recorded to removable media (USB-flash, CD/DVD, etc.)
- **SearchInform FTPController:** data sent over FTP
- **SearchInform Cloud:** incoming and outgoing files of cloud data storages and SharePoint
- **SearchInform PrintController:** data sent to printing
- **SearchInform MicrophoneController:** conversations of employees inside or outside the office.

Control and monitor:

- **SearchInform FileController:** operations with files stored on servers and in shared network folders
- **SearchInform MonitorController:** information displayed on user monitors, keystrokes, contents of the clipboard
- **SearchInform ProgramController:** user activity in different applications.

Work Principle



EndpointController agents shadow copy printed documents, Skype messages, data recorded to removable media, transmitted over FTP and displayed on user screens. Agents also monitor operations with files and send collected data to EndpointController Server.

The server saves all data to the database managed by Microsoft SQL Server.

The database is indexed by Search server which allows fast database search and documents browsing. Indexes are constantly updated and if a security breach is detected AlertCenter will immediately send a notification to the person in charge.

NetworkController and EndpointController: Advantages of Platforms

Complex approach to information security implies using both platforms: NetworkController and EndpointController. If an agent intercepts data a "mirror" does not, then probably traffic is encrypted and sensitive data may leak outside your company in encrypted files. If an agent does not intercept data a "mirror" does, then perhaps it was disabled which also requires immediate attention.

WORKSTATIONS INDEXING SERVER

Search Server indexes new and edited files which makes it available to run full-text search in them. This feature allows monitoring sensitive data stored on user PCs.

Data stored on user workstations is indexed after the agents are installed. The agents log new files and changes made to existing files.

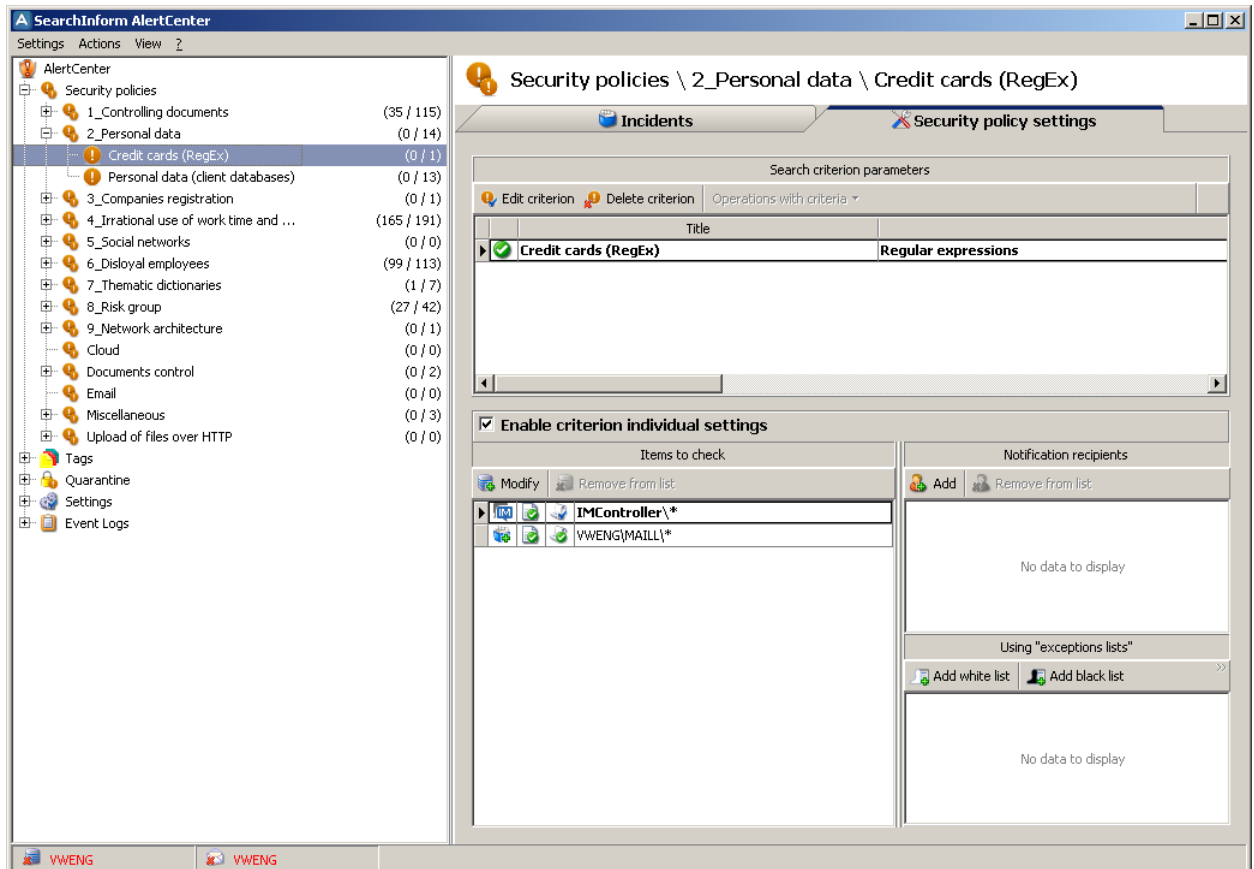
Edited, moved, and deleted files are analyzed in real time.

The scope of files indexed by Search Server extends to 100 file types.

SEARCHINFORM ALERTCENTER

SearchInform AlertCenter is the brain center of SearchInform DLP. It receives data from all software components. If the database of intercepted documents contains key words, phrases or text extracts that match a search query AlertCenter will send a notification to information security officers.

Information security policies (alerts) are created in AlertCenter Client.



You can use the following search types to retrieve sensitive data:

- Search by key words and phrases (stemming, synonym analysis, words space)
- Search by full text or text fragments (similar-content search)
- Search with a dictionary (helps find documents containing words of a specified thematic dictionary)
- Search by digital prints (comparing intercepted documents to the database of known fingerprints)
- Search by the attributes of files and messages (date, size, type, user, e-mail address, etc.)
- Search in databases

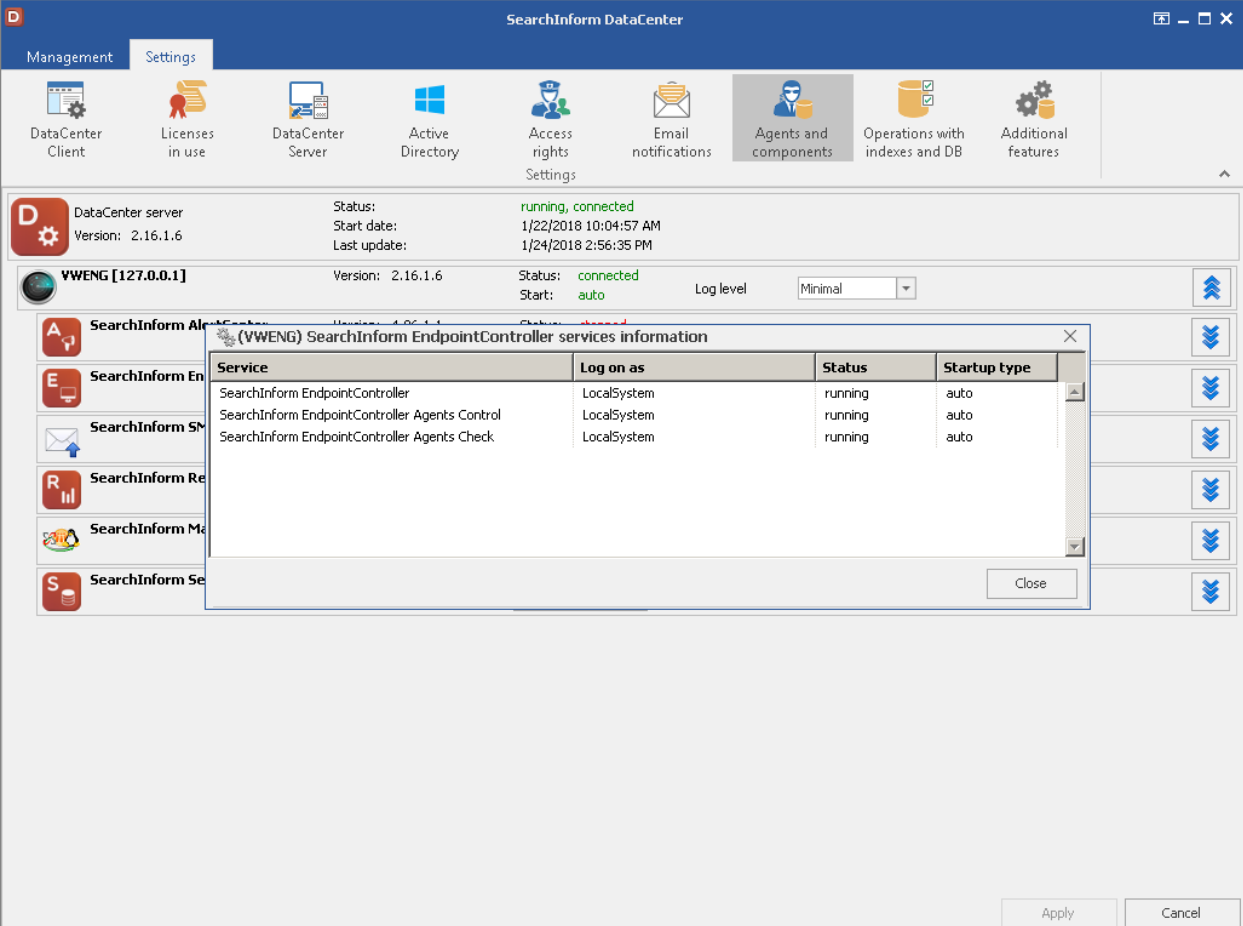
- Searching for password-protected documents
- Complex queries (combining several simple queries with the help of logical operators);
- Search by regular expressions (information is filtered based on data patterns rather than on exact values)
- Statistical queries by quantitative indices (number of sent messages/printed pages/messages in Skype, Lync, Viber, IM, etc.)
- Search by event sequences or sequences with particular duration (password guessing, creation of temporary account, temporary enablement of account, etc.)
- Using synonym rows
- Optical character recognition
- Searching for files with changed extension.

SEARCHINFORM DATACENTER

SearchInform DataCenter is a part of SearchInform Data Loss Prevention and used to automatically or manually control the system performance.

DataCenter:

- Monitors SearchInform DLP services
- Controls free disk space allocated for indexes and databases
- Automatically creates new indexes and databases, sets interception parameters, and deletes indexes if certain conditions are met
- Synchronizes SearchInform DLP with Active Directory
- Restricts access rights to certain information
- Notifies of certain events or malfunctions.



The screenshot shows the SearchInform DataCenter Settings window. A modal dialog box titled "(VWENG) SearchInform EndpointController services information" is open, displaying a table of services. The table has the following columns: Service, Log on as, Status, and Startup type.

Service	Log on as	Status	Startup type
SearchInform EndpointController	LocalSystem	running	auto
SearchInform EndpointController Agents Control	LocalSystem	running	auto
SearchInform EndpointController Agents Check	LocalSystem	running	auto

SEARCHINFORM REPORTCENTER

SearchInform ReportCenter generates reports providing statistics on user activity and incidents.

Functionality:

- Generating reports based on existing patterns
- Library of templates
- Possibility to add new templates
- Switching among different report modes
- Graphical representation of employees relations
- Generating reports and notifications on users and processes activity during working time
- Opening related reports by one click.

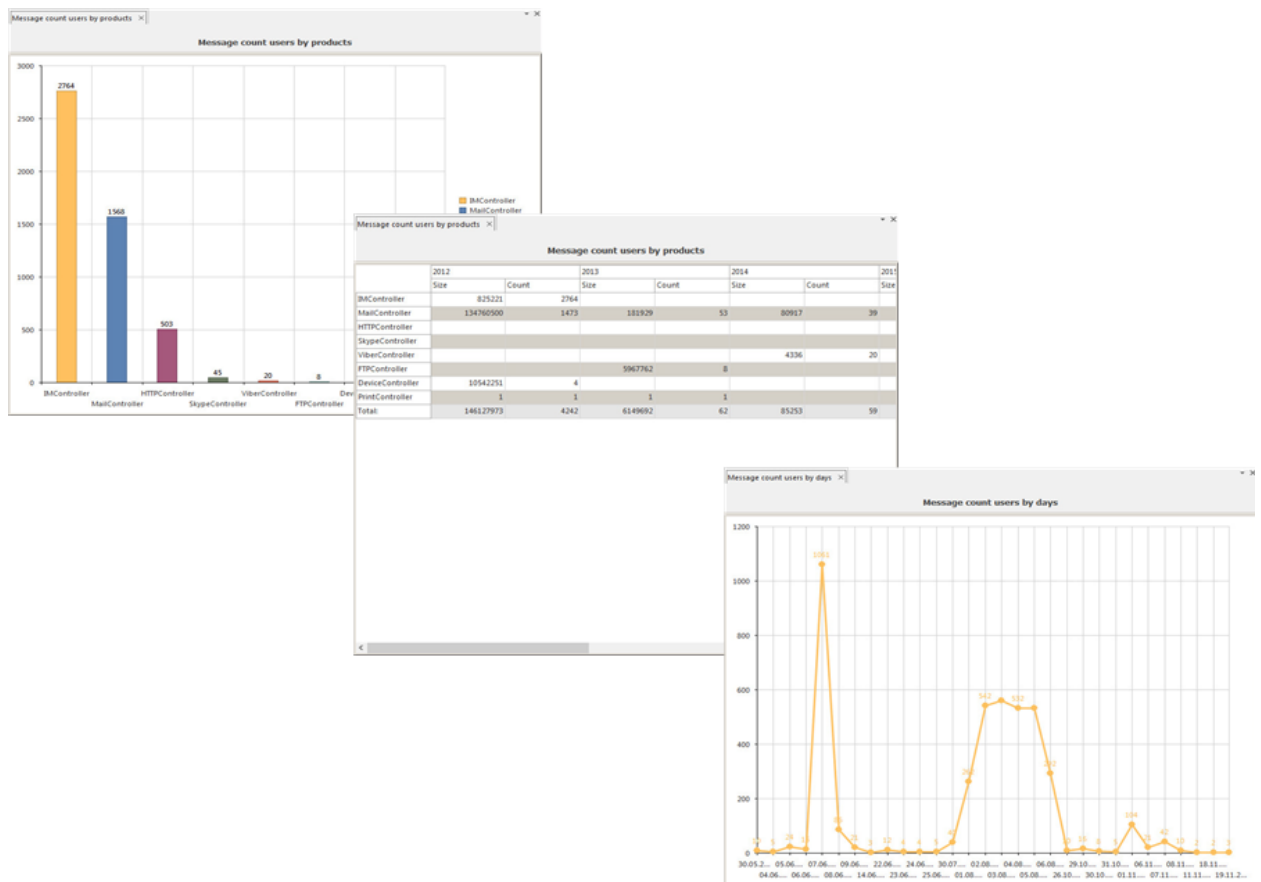
Reports give an idea of how employees use their work time and resources, as well as how they comply with security policies of company:

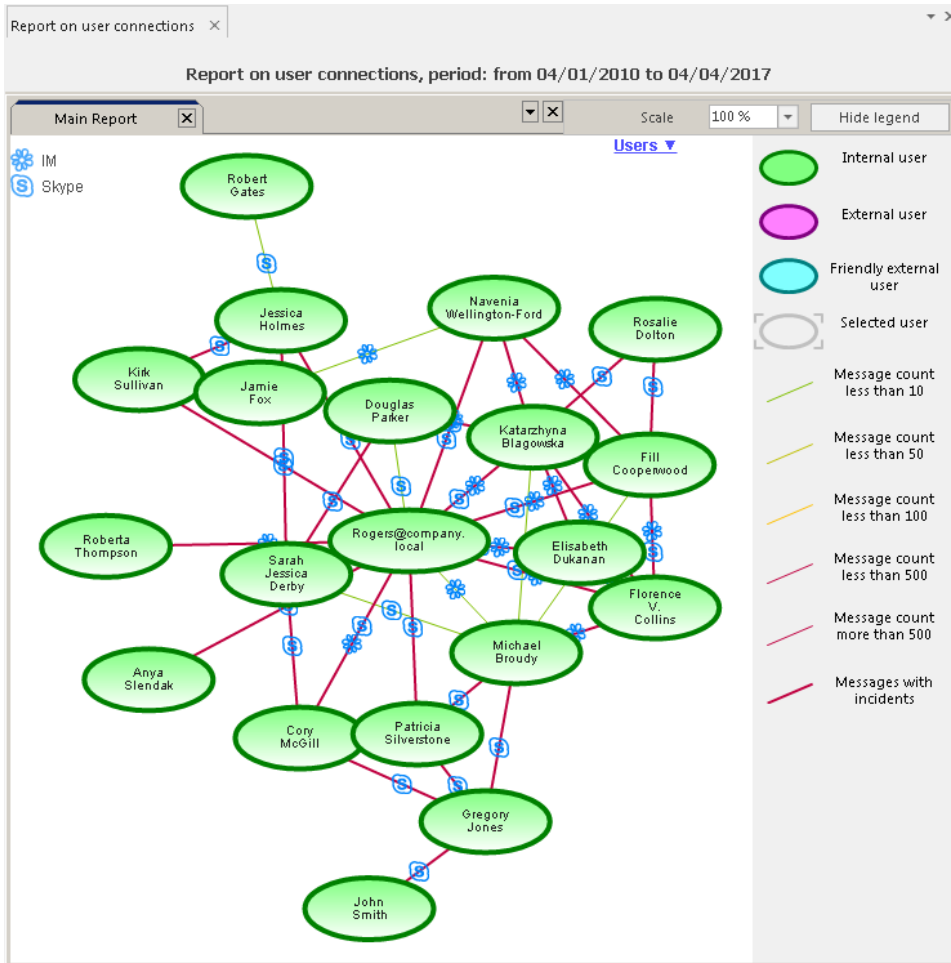
- Most active IM users
- Users involved in the biggest amount of incidents
- Filtering incidents by user groups and associated security policies
- Total time of user work
- Total time of processes activity
- Total time of web sites activity
- Workday duration
- Average daily activity of processes run by users
- Average daily activity of web sites visited by users
- Detailed information on users
- Insufficient user activity during working day
- Continuous activity of users in applications not related to their direct working duties
- Work time log displays work time statistics of selected users during a particular interval
- Work schedule violations, e.g. late arrivals, low performance, etc.
- Filtering incidents by dates and months

- Software installed and changed on user workstations
- Software installation history
- History of agent installation, update, and deletion
- Number of messages on every computer.

Reports can be generated for all protocols and for each separate protocol. It will allow security officers to analyse data on incidents faster and more accurately.

Report can be created in the form of table, diagram, time graph, as well as relations graph, visualization of relations among users.





User relations graph can be useful when investigating data breaches as you can see user contacts inside and outside the company. Every link has its own color which shows the number of messages sent and received. Icons (Skype, mail, etc.) indicate data channels used to transmit/receive data.

ANALYTICAL CAPABILITIES

Analytical module is the most important component of any SearchInform DLP system. Combined use of different search types allows achieving maximum efficiency and reducing expenditures which is extremely important nowadays. SearchInform Data Loss Prevention allows working with all kinds of sensitive data.

The following search types are supported:

1. **Search by words with stemming and synonym analysis.** This simplest search type allows finding documents with queried words and phrases in any word form, their synonyms, located anywhere in the document.
2. **Search by phrases with locked word order and limited distance between words.** This search type allows analyzing documents by phrases (e.g. "first name - last name") or fixed definitions and not just separate words.
3. **Search by attributes.** This search type allows finding documents by their attributes (format, sender name, etc.). You can also use it to monitor activity of certain domain users, IP addresses, e-mail addresses, etc.
4. **Search by regular expressions.** This search type allows tracing all character or word sequences characteristic say for personal data, financial documents or structured records. For example, the system will alert you if someone sends a personal record including data like name, birth date, credit card numbers, phone numbers, etc.
5. **Search by digital prints.** This type of search allows identifying groups of confidential documents and lifting digital fingerprints. The search returns documents containing portions of text from original groups of confidential documents. The main advantage of this search type is high running speed.
6. **Similar-content search.** This search type allows finding sensitive data even if it was heavily edited. You can use text fragments or entire documents as queries. The search will return either identical documents or documents similar in content or meaning. It helps reducing time expenditures.
7. **Complex queries.** Complex queries include two or more simple search queries combined with logical operators (AND, OR, AND NOT). They are used to resolve irregular search tasks.

User Identification

Integration with Windows domain structure enables accurate identification of employees using the following data channels: email, Skype, ICQ, MSN, JABBER, Internet message boards or web blogs, even if they use free e-mail boxes, nicknames, etc. The program can also identify employees who print documents or send them via FTP.

With integration with Windows domain structure, you will easily identify users by their domain name even if they use nicknames.





Revealing Malicious Intents of Insiders

Sometimes employees change extensions of sensitive documents to deceive security officers. Other tricks include sending password protected archives, converting sensitive files to images, etc.

Solution provided by SearchInform allows

- Recognizing text in graphic files and searching in them
- Finding password-protected archives over all possible data leakage channels
- Finding files with changed extension

Controlling Laptops

Employees often take corporate laptops home or on business trips where they can intentionally or unintentionally expose sensitive data to third parties. That is why it is extremely important to control laptops even when they are outside corporate network. All data sent by users is collected and sent to security officers right after laptops are connected to the corporate LAN again.





Controlling User Activity

Researches prove that a typical office employee uses from 30 to 70% of his/her working time for own purposes. Games, chats, and social networks deprive employees of a huge amount of time paid by employers, decrease efficiency and company's competitiveness. Monitoring adherence to the working schedule and employees' activity during the day, as well as analyzing their work in different applications helps strengthen security and encourage employees for more efficient time usage.

Data Flow Control

Architecture

All system components have client-server architecture.

Server side includes two platforms: NetworkController or EndpointController. Client side includes applications used to search and view captured data (SearchInform AlertCenter, SearchInform ReportCenter, SearchInform Client).

Single search-analytical engine allows using all of the above-mentioned search possibilities in full.



Users can expose sensitive information in email messages, which is very difficult to control. Insiders are well aware of this and a significant share of data leakage goes exactly this way. At the same time, it is very difficult to find anything in the ocean of email messages.

SearchInform MailController intercepts users' email traffic on a protocol level or by means of agents installed on user workstations. All intercepted messages are indexed which allows fast database search.

It transfers all intercepted e-mail messages (message body and attached files) to SQL database, indexes them, creating a unique corporate email archive. Even if your corporate mail server fails, which is indeed a very unpleasant situation entailing significant losses, you can use intercepted data as a full-fledged backup of your email base.

SearchInform MailController

- **SMTP** (outgoing e-mail over mail client)
- **POP3** (incoming e-mail over mail client)
- **IMAP** (including *IMAP Compressed*)
- **MAPI** (including *RPC over HTTP*)
- **NNTP**
- **HTTP(S)** (*Exchange Web Services* – incoming and outgoing mail, *Kerio Outlook Connect* – incoming and outgoing mail, *Outlook Web App* and *Outlook Web App light* – outgoing mail, *Zimbra Web Client* – outgoing mail, as well as incoming and outgoing e-mail of web mail servers *yandex.ru*, *tut.by*, *gmail.com*, *outlook.com*, *mail.ru*, *rambler.ru*, *office 365*, *ukr.net*, *yahoo.com*, *qip.ru*, *Google Sync*).

Integration with:

- Mail servers: **Microsoft Exchange**, **Lotus Domino**, etc.
- **Microsoft ISA / Forefront TMG** and other proxy servers working over **ICAP**.



SearchInform IMController

Controlled protocols:

- **OSCAR (ICQ/QIP)**
- **XMPP** (Jabber, Google Talk)
- **MMP** (Mail.ru Agent)
- **MSN** (MSN/Windows Live);
- **HTTP IM** (Facebook, LinkedIn, Google+, etc.);
- **SIP** (Microsoft Lync, X-Lite, etc.)
- **Gadu-Gadu** (Gadu-Gadu)
- **YAHOO** (Yahoo messenger)
- **Viber** (Viber desktop)
- **Microsoft Lync**
- **Telegram** (Telegram Desktop)
- **WhatsApp** (WhatsAppDesktop)

Instant messengers and social networks (ICQ, Facebook, LinkedIn, etc.) are no longer an entertainment medium they used to be, but a full-featured tool for business communications and transfer of valuable information. However, IM clients may be used by insiders for malicious purposes, i.e. sending sensitive data to untrustworthy parties.

SearchInform IMController intercepts messages sent over popular IM clients.

It saves all messages to the database where you can search for data using SearchInform search engines (morphology, synonyms, similar-content search, etc.).

You can filter intercepted messages, e.g. view communication between selected users during a particular time interval.



SearchInform HTTPController

Social networks and web blogs have been rapidly developing in recent years. On the one hand, they help you recruit staff, find potential business partners, etc. On the other hand, these new ways of communication can make your business more vulnerable to security threats. Employees can use social networks, blogs, and chats for illegal actions and pose threat to company's reputation and financial activity.

SearchInform HTTPController intercepts files and messages sent over HTTP, indexes all intercepted messages and provides full text search in them. This allows tracking files and messages sent to web-blogs, chats, via webmail services or browser IM clients.

With HTTPController, you will be able to control your staff and their communication during working hours.

Data sent over HTTP(S) is controlled (POST):

- Email over web interface;
- Web blogs
- Web forums
- Contact forms
- Web chats
- Social networks (Facebook, Google+, LinkedIn, etc.);
- Browser IM clients (ICQ, MSN, QIP, etc.).

Search engine GET requests are also intercepted.



Skype has become a full-featured tool for business communication and information transfer. It offers traffic encryption which makes Skype one of the most secure communication channels.

However, it may also be a serious threat to a company. Having a reputation of being the most reliable VoIP service, Skype is often used by insiders to transfer sensitive information outside the company. Trying to protect their companies from possible data leaks, some employers just disable this data channel, which creates additional obstacles for business communication.

SearchInform SkypeController is used to intercept and analyse Skype traffic: voice and text messages, SMS and files sent over Skype.

SearchInform SkypeController

SearchInform SkypeController is used to capture and analyze Skype traffic:

- Text messages
- Files
- Voice sessions
- SMS.



SearchInform DeviceController

Additional features:

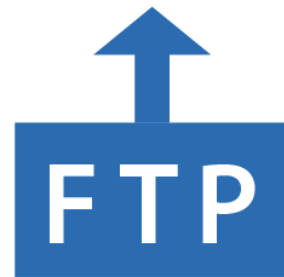
- Complete and partial blocking of data storage devices, e.g. read-only mode is allowed while all other operations are disabled (recording, copying, etc.)
- White/black lists of devices
- Encryption of data sent to USB
- Limit of access to folders and disks.

The easiest way to steal sensitive data is to copy it from corporate LAN to removable media: CD/DVD/USB.

Sure you can block USB/Firewire ports and disable CD/DVD burners... but is this really the best way to protect your information? How will it affect your team and their output?

SearchInform DeviceController is a software unit used to intercept data recorded to removable media. Intercepted data is saved to a database where it becomes available for full-text search and analysis.

It also allows restricting access to different types of removable media: scanners, modems, printers, or tablets.



SearchInform FTPController

FTPController monitors documents uploaded or downloaded over FTP and secure SSL connection.

File Transfer Protocol (FTP) is commonly used to download software, upload websites, and send files to FTP servers.

FTP servers are popular among users and can be accessed by virtually anybody including insiders and careless employees.

SearchInform FTPController allows intercepting all inbound and outbound FTP traffic. It saves all intercepted information to a database and makes it available for further search and analysis.



SearchInform PrintController

Any employee can print sensitive data and take it outside the office. Printers can also be used for private business or personal goals that have nothing in common with the working process.

SearchInform PrintController monitors local and network printers and discovers sensitive information in printed documents. It monitors printed-out documents, indexes them and sends them to a database.

History feature is supported which means you can always view who printed the document, when, and how many copies were made.

By monitoring every printed document, you can not only prevent data leakages but also estimate if the printers are used as intended.



SearchInform MicrophoneController

MicrophoneController is used to record conversations in office or on business trips. Voice is recorded with the help of any detected microphone (headset, laptop, webcam, etc.) and saved in the database. You can listen to the recorded data and filter it by attributes.

This software application is an essential component when investigating data breaches.

MicrophoneController can be installed on any workstation. Voice is recorded unnoticed to users.

You can set up the following modes:

- Recording speech only or all sounds
- Recording voice inside or outside the office
- When recording voice – changing upper and lower values of Voice Activity Detection algorithm (recognizing human speech among background noise or silence)
- Duration of recordings
- Level of noise reduction
- List of processes that trigger recording.



SearchInform MonitorController + Keylogger and CameraController

Office Internet can be a benefit and harm at the same time. Users may be tempted to watch news or entertainment programs and ignore their work.

SearchInform MonitorController intercepts data displayed on user monitors. The solution is supplied together with keylogger module which allows intercepting keyboard strokes.

It captures screenshots at regular intervals, intercepts key strokes in various applications, content of clipboard, saves them to a database managed by Microsoft SQL Server. You can monitor visual data displayed on one or several user screens in real time.

If there is any webcam connected to the computer, it is possible to identify a person authorized in the system, presence of an employee at the workplace, as well as his/her actions during a day. The LiveCam mode allows connecting to a webcam and watching activity in the office live.

The product can be installed on any workstation. Screenshots are captured unnoticed to users.

MonitorController and Keylogger helps understand whether employees waste their time at work or not, as well as how they comply with security policies of company.

Screenshots can be taken and video can be recorded according to the specified conditions.

LiveView and LiveCam modes.



SearchInform FileController

File servers store a large number of documents including confidential ones. Employees may get access to sensitive data and expose it to third parties.

FileController logs any operations with files by means of agents installed on user workstations (opening, copying, changing, etc.).

FileController monitors the following operations: creating, reading, recording, deleting, renaming, running, etc.

Files are monitored at the level of file servers and user workstations.



SearchInform CloudController

Today's popularity of cloud services is explained by ongoing growth of information technologies and higher Internet speeds. Data stored in cloud is available to users no matter where they are and what devices with Internet access they use.

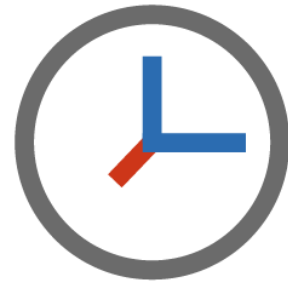
Advantages of such services are obvious. Employers can easily imagine amounts of money that can be saved on equipping their employees with computers, buying software licenses and paying to IT experts.

However, your information is stored on a remote computer. Although all services are doing everything to keep your data confidential, nobody guarantees protection from data leaks ensured by your own employees.

SearchInform CloudController is used to monitor incoming and outgoing data of cloud services. It supports the following services:

- Google Drive
- OneDrive
- Office 365
- Dropbox
- Evernote
- Yandex Disk
- SkyDrive
- cloud.mail.ru
- iCloud Drive
- DropMeFiles
- Amazon S3
- OwnCloud
- Pcloud
- OziBox
- MediaFire
- OpenDrive
- 4shared
- Box
- Syncplicity
- CloudMe
- MiMedia.

Files sent via MS SharePoint are also controlled.



SearchInform ProgramController

Probably every employer would like to know how much time employees spend on work, why and how often they browse web content, what emails they send, etc. This information can give a basic idea of staff loyalty and diligence.

SearchInform ProgramController is used to monitor user activity in launched applications and on web sites during the work day. The captured data is saved to a database after which it becomes available for search and analysis.

- ProgramController can be installed on any workstation.
- Activity is monitored in stealth mode.
- It is possible to monitor particular processes and web-resources
- Search of captured data by user, computer, MAC and IP address, processes, etc.

SEARCHINFORM DLP Advantages

SearchInform DLP is developed to work in large corporate environments. It has the following advantages:

- **Easy to integrate.** SearchInform DLP can be deployed in a company within several hours. Our customers won't need any outside help to do it. It means they won't need to show sensitive documents to third parties. The deployment will not affect your corporate information system.
- **End-to-end solution.** SearchInform DLP controls all data channels in a company. Multicomponent architecture allows selecting only those units you really need.
- **Full control of information sent over Skype** (voice and text messages, SMS and files).
- **Laptop control** allows monitoring user activity outside the office – at home or on business trips
- **Integration with Windows domain structure.**
- **Powerful analytical module** helps quickly and efficiently tune notification system without the help of third parties. Minimum labor expenditures are needed to analyse data flows.
- **Proprietary similar-content** search allows finding documents similar to the original in content and meaning.
- **User relations chart** allows automatic detection and analysis of user relations in and outside the office. This feature is crucial when conducting internal investigations.
- **User access rights differentiation.** Setting up permissions to access intercepted data.
- **Workstations and shared folders control.** This feature allows finding sensitive data where it should not be stored.
- **Database of intercepted documents.** Database allows restoring the sequence of events in the past.
- **Own deployment department and training center.** Rich experience of working with more than 1500 different companies helps quickly create unique security policies sets for your type of business.

CONTACT DETAILS

BELARUS

Tel.: +375 29 649 77 79

Email: ab@searchinform.ru

BENELUX

Tel.: +31 6 44 78 62 93

Email: benelux@searchinform.com

BRAZIL

Tel.:

+ 55 11 43 80 19 13

+ 55 11 98973 2037

Email: v.prestes@searchinform.com

EMEA

Tel.: +44 0 207 043 7152

Email: sy@searchinform.com

KAZAKHSTAN

Tel.: +7 495 721 84 06, ext. 137

Email: d.stelchenko@searchinform.ru

LATAM

Tel.:

+54 11 5984 2618

+54 911 5158 8557

Email: r.martinez@searchinform.com

RUSSIA

Tel.: +7 495 721 84 06

Email: info@searchinform.ru

UK

Tel.: +44 0 20 3808 4340

Email: uk@searchinform.com