

SearchInform DLP

Data Loss Prevention and Insider Threat Security



SearchInform Today

- Over 2000 customers in 17 countries
- Over 11 years on the DLP market, 22 years in the IT industry
- SearchInform DLP monitors over 1.200.000 PCs
- Experienced deployment and support team
- In-house Training Center



searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Internal Threats

More and more companies and individuals become targets for malicious actors. The main sources of internal threats are:

Malicious insiders:



Privileged user abuse, employees using their high access levels to steal sensitive data.

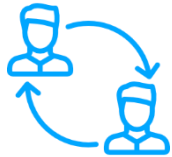


Harmful activities: kickbacks, forgery of documents, drug abuse and distribution, terrorist recruitment, bullying, bashing the company on the Internet, etc. All these may cost a company money and/or reputation.

Internal Threats



Negligent insiders. Such employees may store their password on a piece of paper stuck to the computer screen, plug in a USB flash drive found on a parking lot, send sensitive data to a wrong email, etc.



Exploited insiders can be lured into providing classified information or even making payments to attackers' accounts as a result of blackmailing, social engineering, and other pressure.

Solution

A software solution to tackle these problems must have the following features:

- Monitors in stealth mode
- Controls virtually all information channels
- Includes repository of captured data in order to perform investigations
- Performs monitoring both inside and outside the office
- Detects sensitive content in documents of virtually all types
- Allows you to monitor user screens and employee conversations retrospectively or in real time.

SearchInform DLP Fits the Bill

Each of the components controls its own data channel. The system reveals the paths data travels through and makes all communications transparent.



Overview

SearchInform DLP protects your business against internal threats from all angles:

1. Controls all flows of information
2. Captures the content of messages and attachments
3. Notifies about security policy breaches
4. Helps to investigate incidents and prevent data leaks

Main objective of the solution is to discover data leaks and harmful activities at the planning stage and prevent them from happening.

How It Works

The software controls:



Communication channels

Email, messengers,
Cloud storages, etc.



Employee activity

Computer activity, transfer
of data to USB sticks,
document printing



Data at rest

Data stored in network
folders, on PCs, etc.

DLP Components



MailController

Captures all incoming and outgoing email sent via web browsers (Gmail, Yahoo, Hotmail) or mail clients (Outlook, etc.)



IMController

Captures chats in social networks (LinkedIn, Facebook, etc.) and instant messengers (MSN, Jabber, ICQ and others), as well as incoming and outgoing messages from other popular sites



SkypeController

Captures all communication via Skype:

- Chats
- Calls
- SMS
- Files

DLP Components



HTTPController

Captures files and messages sent over HTTP(s) and lets you control:

- Web forums
- Feedback forms
- Browser IM clients
- Web blogs
- Web chats
- Social networks



FTPController

Captures data sent or received via FTP, including encrypted connection (FTPS)



CloudController

Monitors Cloud inbound or outbound traffic:

- Google Drive
- Just Cloud
- Mega
- OneDrive
- Evernote
- Dropbox

DLP Components



MonitorController

Takes screenshots and records video of workstation screens. Operates in several modes:

- Takes screenshots on schedule or on event, like program/process start
- Monitors desktops in real time
- Records screen videos



MicrophoneController

Records employee conversations in the office and on business trips via any detected microphone, built in or plugged in:

- Non-stop recording
- Recording can be triggered by a program/process launch
- Recording can be triggered by human speech
- Live sound broadcasting

DLP Components



PrintController

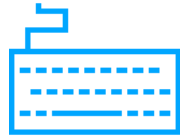
Monitors the content of documents sent to printers regardless of the printer model, as capturing takes place at the OS level



DeviceController

Captures the data transferred by users to external devices: scanners, modems, smartphones, tablets, memory sticks, etc. The module detects all occurrences of such devices being plugged in

DLP Components



KeyLogger

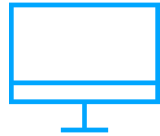
Captures key strokes (logins, passwords, etc.) as well as data copied to clipboard. Lets you track the credentials used to access potentially dangerous resources



ProgramController

Collects the data on applications run by employees during the day and time spent running the applications. The module detects whether the user actually operated the application or the application just ran unattended

DLP Components



Workstation Indexing

Allows you to detect occurrence, copying, movement, and removal of sensitive data on user workstations in real time.



FileController

Monitors the operations on file servers and in shared network folders. Logs all operations with files: opening, copying, modifying, deleting, etc.

DLP Architecture

All system modules are based on two platforms. Best results are achieved when they are used in combination:

NetworkSecurity

Control at the network level

Mirrors traffic at the level of the corporate network (switch)

Mail, IM, HTTPS, FTP, Cloud, Active Directory Controllers

EndpointSecurity

Control at the workstation level

Captures employee activity by means of agent-programs installed on workstations

Mail, IM, Skype, Device, FTP, Print, HTTP, File, Monitor, Microphone, Cloud Controllers

DLP Analytical Capabilities

There are 2 main criteria based on which DLP systems can be evaluated: number of channels controlled by the system and the system's analytical capabilities. In order to detect suspicious activity in captured data, SI DLP uses **7 types of search**:

- Word search
- Phrase search
- Dictionary search
- Attribute search
- Similar content search
- Regular expression search
- Digital fingerprint search

These analytical capabilities of SearchInform DLP allow one information security officer to control up to **1000-1500 employees**.

DLP Analytical Capabilities

The system lets you combine the single queries to create complex search algorithms that form the information security policies. SI DLP includes **over 250 predefined security policies**:

- **Universal security policies** for detecting kickbacks and bribery, negative attitudes among the staff, etc.
- **Industry specific policies:** agriculture and forestry, mining, manufacturing, gas-, energy-, and water supply, construction, trade, transport and logistics, information and communications, finance activity, insurance, state management and defense industry

What Happens After Incident Detection



As soon as the system detects a suspicious activity or a policy violation, it sends **a notification** to the designated security officer who then initiates an investigation. Analytical capabilities of the system allow you to restore all necessary details and prevent data leaks.

SI DLP also generates **over 30 reports**, which help optimize work processes:

- For a supervisor to increase employee productivity
- For an HR to improve work discipline
- For the IT department to automate hardware and software control

Technical Advantages

- 1 Full integration with Windows domain structure**

DLP unambiguously identifies user accounts and computers regardless of Skype accounts or mailboxes being used
- 3 Computer screen capture**

Shows who viewed what information during the work time. Records videos or takes screenshots of screen activity and lets you monitor user screens in real time

- 2 Archive of captured data**

The system saves all captured data to an archive. You can always recheck the stored data against new information security policies
- 4 Employee conversations under control**

The software records employee voices inside and outside the office. By enabling the Live Sound mode, you can listen to employee conversations in real time

Technical Advantages

5 **Transparency of connections inside and outside the company**

The system analyzes internal and external social connections of employees. The map of interactions helps to lead investigations

7 **PC and network resources under control**

Information security officers are able detect sensitive data in locations where such data is not supposed to be stored

6 **Protection from system administrators**

Event monitoring of Active Directory logs allows you to detect suspicious activities performed by system administrators

8 **Reports on software and hardware**

The system facilitates stock-taking and software monitoring. It allows you to optimize IT-department performance and avoid unnecessary expenses

Why SearchInform DLP



Installation takes just 2-3 hours

And this can be done by your IT staff. You don't have to disclose your internal documents and processes



The deployment will not interfere with your work processes

DLP installation does not require any changes in your local network structure. Thus the product deployment will not cause any downtime or change established processes.



SI DLP protects your data offsite

It operates not only at the level of the local network but also at the level of each separate computer. The software secures your data even when employees work from home or while on business trips.

Why SearchInform DLP



Flexible licensing

SearchInform DLP is a multi-component system. The customer can purchase the full software suite or selected modules



Constant support of the deployment department

SearchInform teaches how to operate the software, helps to work out security policies, provides consulting on the interception analysis and keeps you updated on the new software features and capabilities



Free trial version for 30 days

You get to test the product and understand its value for your business before you buy it. Full functionality and training are provided during the trial

START YOUR FREE TRIAL TODAY!