

It's your power  
over information



## Search & Security

---

© SearchInform Technologies Inc.

It's your power  
over information



## INTRO

Today, when information is as valuable as it is and companies cannot afford having it stolen, lost or disclosed, information security becomes the critical element and basically the driving force in most business processes.

All potential threats can be divided into external or internal ones. External threats include unauthorized programs (such as worms, Trojan viruses, spy-programs, etc.), and there is really no universal solution that would protect your company from all types of threats, that's why there are so many specialized programs dealing with each particular problem.

However, it's the internal threats that usually make companies most vulnerable. And one of the most probable variants of information security violation is the deliberate theft of confidential data by authorized users (or so called insiders) via e-mail. This paper will deal with the problem of internal information threats and touch on a possible solution that lies in the teamwork of search and security technologies.

It's your power  
over information



## THE ROOT OF IT ALL

E-mail has long seized to be merely means of communication between people living far away from each other, it has become an indispensable tool of information exchange in all modern business processes.

An active e-mail user sends and receives dozens of e-mail messages daily, let alone any small-scale company. Business correspondence with clients, commercial mailing, internal company communication, employees' personal letters from personal accounts, as well as all incoming correspondence – the list could go on forever, really.

The software market offers a large variety of e-mail traffic interception programs. So, at first one might question the need for new products in that field. Yet if you take a closer look, most programs don't live up to the needs of potential customers. Some can't manage large flow of messages that is so typical in large enterprises; others simply store the intercepted messages making it extremely hard to find something in this haphazard storage and thus dismissing the value of information.



## SOLUTION

SearchInform MailSniffer from SearchInform Technologies is a multifunctional tool for organizing work with e-mail both on a separate computer and within the local network. The software intercepts all incoming and outgoing e-mail traffic, indexes it and places it into a database, making the stored messages available for search. The client-server architecture and the possibility to process large volumes of information make MailSniffer ideal for corporate use.

In order to properly organize e-mail interception, MailSniffer can be installed on the internet server and on a separate computer, to which all e-mail traffic will be redirected by the **mirror switch**. The latter is even more preferable, as in this case, SearchInform MailSniffer would not create additional pressure for already overloaded internet server.

The software comes with a full package of technical documentation, including step-by-step installation guides. Because mail interception happens on the "hardware" level, it does not depend on the type of the mail client used. We should note however, that the traffic coming through encrypted non-standard protocols does not get intercepted.

The interception and indexing of the outgoing and incoming traffic starts right from the moment the software is installed. The search will be conducted only within the intercepted mail. If you want to search in the messages, received or sent before the installation of MailSniffer, you can use the feature of importing the existing mail database from the popular mail clients (such as Outlook, Outlook Express, the Bat, Mozilla Thunderbird, Eudora, etc). If you did not find your mail client in the list of supported mail clients, it can be easily resolved – MailSniffer has a function of importing messages in .MSG format.

Upon installation a primary MailSniffer installation wizard will launch. It is activated with the first launch of the application and helps the user to correctly set up the system for incoming and outgoing e-mail interception.

Being an information interceptor, MailSniffer falls under the category of the information security software. However, besides ensuring that the confidential information does not flow in a wrong direction, MailSniffer also provides the user with a manifold of various possibilities for organizing the work with e-mail. Taking a closer look at this software, we will discover that instead of a regular spy-application MailSniffer is a comprehensive system for mail account management with rich search possibilities.



## A MORE DETAILED LOOK

Information, especially that hidden from the common access and use, has always been highly valued. A constantly increasing interest in information security software can be explained by an ever growing information volume and the ease of accessing it. If only a few decades back the data stored on magnetic tapes or on a separate computer was extremely hard to access and barely few people had enough technical skill to do so, today computers are usually connected to company or home networks and almost everybody has access to the Internet. Email being one of the most common activities we engage into on the Internet, it is also one of the most common means of confidential information disclosure. Whether it is commercial information, your personal correspondence or developments, MailSniffer will intercept all incoming and outgoing messages and you can easily track and prevent all attempts of information theft.

The search capacities of SearchInform MailSniffer, the name of which speaks for itself, correspond with those of SearchInform search system. This means that the user gets a full-fledge full text search tool that performs search with due consideration to stemming, phrase search with consideration to distance between words, as well as "search for documents similar in their content to the query". The peculiarity of this unique function lies in the query size – not only a word or a phrase, but also a large paragraph or even a whole letter can be easily used as a query. Next the program analyzes the whole variety of words occurring in the letters and organizes the letters based on their relevance to the query in the list of results (specifying the percentage of relevance at side). If the system shows 100% relevance, it means that a complete duplicate of the query letter has been found. That will most likely be one of the letters sent to more than one contact from the mailing list.

Also implemented in the program is full text search in all message attributes and attachments (even archived ones). At first there seems to be nothing unique in these features, as a lot of desktop search engines conduct search in mail client databases. Yet SearchInform MailSniffer, having found the needed data, not only provides the file attached to the message, but also connects it with the letter itself. The user can view when and to whom the letter was sent. Setting time intervals can narrow the



search area, save the time the program would normally waste on searching and the time the user would normally spend on browsing irrelevant results.

Apart from that, MailSniffer is also a convenient tool for monitoring your employees' work performance. If for personal use such measures may be considered unethical, it is more than appropriate for any office, as bosses should be able to tell, how diligently their employees work and how rational their time use is. MailSniffer's 'correspondence history' function allows you to track all mail exchanges between 2 mail addresses. You just need to select one of the messages, click the 'correspondence history' button and you will see the entire correspondence history in chronological order. If one of the recipients changed his/her e-mail address in the course of exchanges, then the function of 'search for similar' will come in more than handy. Using one of the dialogue paragraphs as your query, you will end up with all the messages containing this paragraph, and therefore related to this e-mail exchange. Except for the monitoring function, this feature also allows to recollect the events throughout an e-mail exchange extended in time.

The client-server architecture of the application along with its internal access rights differentiation allows you set the access rights to the information from company's mail database with maximum precision. The system is usually set by the system administrator. Using application's functional, it is also possible to set the flow of mail in such a way that the head of each department will be able to see the e-mails sent or received by the employees in his/her department, while subordinates will only see their own correspondence. Though, the system's flexibility allows this hierarchy to be arranged in a different way. For instance, the heads of adjacent department can see the e-mails of both the departments' employees, or even the correspondence of certain employees of the other departments. After all it is obvious that just as well as a sales manager should not be reading the CEO's mail, the correspondence of the accounting department should not be made public.

At interception the information from all letters gets indexed and stored into a database, a so-called storage. So when deleting a letter from the mail client (either accidentally or intentionally), all data it contained will still be available for search.

Even if the corporate mail server crashes, which is obviously never a pleasant thing to deal with and entails large time losses on recovering, the

It's your power  
over information



data intercepted by MailSniffer will play the role of a back up database of the whole enterprise.

SearchInform MailSniffer is the first product in the line of security solutions from SearchInform, that is also a powerful tool for organizing work with the mail database of an large enterprise. This, in essence, is a multifunctional tool for organizing the company's work with electronic correspondence, rather than a mere e-mail message interceptor.

The messages are intercepted based on an IP address, a set of IP addresses, or MAC-addresses of network adaptors. Such interception filter allows the user to set the work of the program with more detail. All intercepted messages get placed into a storage. This not only allows the user to conduct search in deleted from the mail client messages, but also creates an archive of the company's whole database. The search capacities that MailSniffer acquired from its bigger brother SearchInform provide the user with fast and quality search in the whole mail database. Unique *similar search* feature adds on to and extends these capacities, making search for the needed information even simpler. Full control over correspondence that the program provides gives you full control over your employees' correspondence.

**This program with its powerful search engine and rich management capacities, user access rights differentiation and client-server architecture will most of all interest the corporate user.**