

It's your power  
over information



## Search Technologies to Provide Information Security

---

© SearchInform Technologies Inc.



Today the problem of securing the information contained in the enterprise's data space becomes more and more critical. Most of the time it's not just company's corporate data, but rather the information hidden from common access that is most valuable.

Specialists in the field of information security distinguish two types of potential threats:

- external
- internal

Systems providing security from external threats prevent unauthorized programs (such as worms, Trojan viruses, spy-programs, etc.) from running and block external attacks on system resources and processes. Yet in addition to all these, any company's security system is threatened from within, and it's the internal threats of information disclosure that make companies most vulnerable.

**What are these internal threats and how can you rid your enterprise of them?** This paper will deal with this problem and a possible way out of it.

### **Insiders: how and why**

The danger lies in the fact that most employees have access to the organization's repositories of information and are exempt from such network defenses as anti-virus programs, firewalls, even e-mail filters. Information leak is not always incompetent leaders' or unqualified staff's fault, more often the software installed on the enterprise and its shortcomings are to blame. The most probable variant of information security violation is the deliberate theft of confidential data by authorized users (insiders). Such things as conflict with the management, with fellow staff, trivial dissatisfaction with the salary may trigger the leak of confidential information to competitors as well as an attempt to destroy it.

### **The problem with your standard security systems is...**

On the market there's quite an extensive array of corporate applications designed to solve the problem of information security. Developers create not only complex means of information security but also systems oriented on withstanding certain groups of threats.

When creating an information security system the developers try to extend its functional to the maximum so as to work in a variety of fields. Even operation systems today contain security functions designed to increase the enterprise's safety level. But this "universality" is unacceptable when speaking of important and valuable data. A universal security system becomes useless in corporate networks where internal threats (insiders' activity in particular) prevail.

That's why most people responsible for their organization's information security prefer to use external security systems rather than those inbuilt into a standard operation system.

### **What does the market say?**

Security market sees an ongoing growth in the number of security tools and large-scale monitoring systems designed to prevent internal threats. All of them strive



to provide total control and consequently all aspects of information safeguarding and protecting for the entire organization.

One of such tools that has already gained a high degree of popularity on the market is a security solution from SearchInform Technologies, a company well-known for developing a corporate full text search engine called *SearchInform*.

It's next to impossible to eradicate the risk of an insider gaining access to unauthorized information with the goal of theft and later disclosure to a third party. Solution from SearchInform Technologies lets you fully control this process from the ground up.

### How it works

The first stage is taken care of by **SearchInform Security Server**, which enables the user to work both with his PC and in the local network both with open and confidential information while preventing unauthorized data from appearing where it's not supposed to. **SearchInform Security Server** in real time mode monitors all the file transactions and modifications taking place on user computers.

The fact that this system is based on search technologies takes it to a significantly higher quality level. All information in the local network gets indexed and becomes available for fast and quality full text search. While at that, the search itself is conducted not only by file names, but also by their contents. The search engine used in **SearchInform Security Server** acquired full functionality of SearchInform corporate search system. Quick indexing, support of over 60 file formats, correct work with databases, caching system – to list only a few of its advantages.

Search module lets you conduct information search in the data received from all the computers in the local network using a set list of keywords, phrases, or even text extracts. The information you get as a result will contain information on new, modified and deleted files containing key words; an alert system will send these results to the organization's info security pro's either through messenger, by e-mail or any other way convenient to the user.

### What if they use internet?

Control of internet traffic is of as high importance as all of the above since it has hitherto been the least controlled field. That's the weakness insiders exploit to the fullest – Internet forms the bulk of how confidential information gets disclosed. **SearchInform Traffic Analyzer** is designed to monitor the whole of Internet-traffic. With its help you can't track not only all the http-traffic and logs of such instant messaging programs as MSN, Trillian, ICQ, etc., but also all the e-mail correspondence. It doesn't matter which e-mail client the insider is using, even if the letters were sent through free e-mail clients (like Hotmail.com or gmail.com, for instance) rather than through the corporate mail server.

Like in SearchInform Security Server, all the information gets indexed and is stored on the server for a certain period of time and is available for conducting full text search in it during that time. An alert system is set in a way that when a certain keyword or phrase appears in search results on a user computer, the corresponding information is sent to the organization's information security person.

It's your power  
over information



### **And the e-mail?**

Electronic mail control is taken care of by **SearchInform Mail Sniffer** application. It intercepts all e-mail traffic on the protocol level, so it doesn't really matter how exactly the e-mail was sent. Full text search by key phrases is conducted not only in the heading and body of the letter, but also in the files attached to it. For instance, this way you can easily track who, how and when tried to send confidential information to the external sources as well as see which of your employees are sending their resumes to the competitors.

### **So what?**

Security solutions from SearchInform let you process both open and confidential information while preventing unauthorized modifications and information leak to the outside sources. The system tracks the whole of information flow both on the user computer, in the local network and the information that goes into Internet. This helps to protect the organization from the harm that insiders may cause – a domineering threat, which poses an insurmountable impediment to the proper functioning of any organization and can easily cause havoc in the company's information management system. Security system from SearchInform Technologies with an inbuilt powerful search module is a new approach to this problem that can rids the enterprise of the headache related to the information leak and disclosure.