

## Ultimate control over data leaks

Does your company use various data transmission channels?

Are there any sensitive documents your employees have access to?

You think all your employees are loyal?



# SecureTower

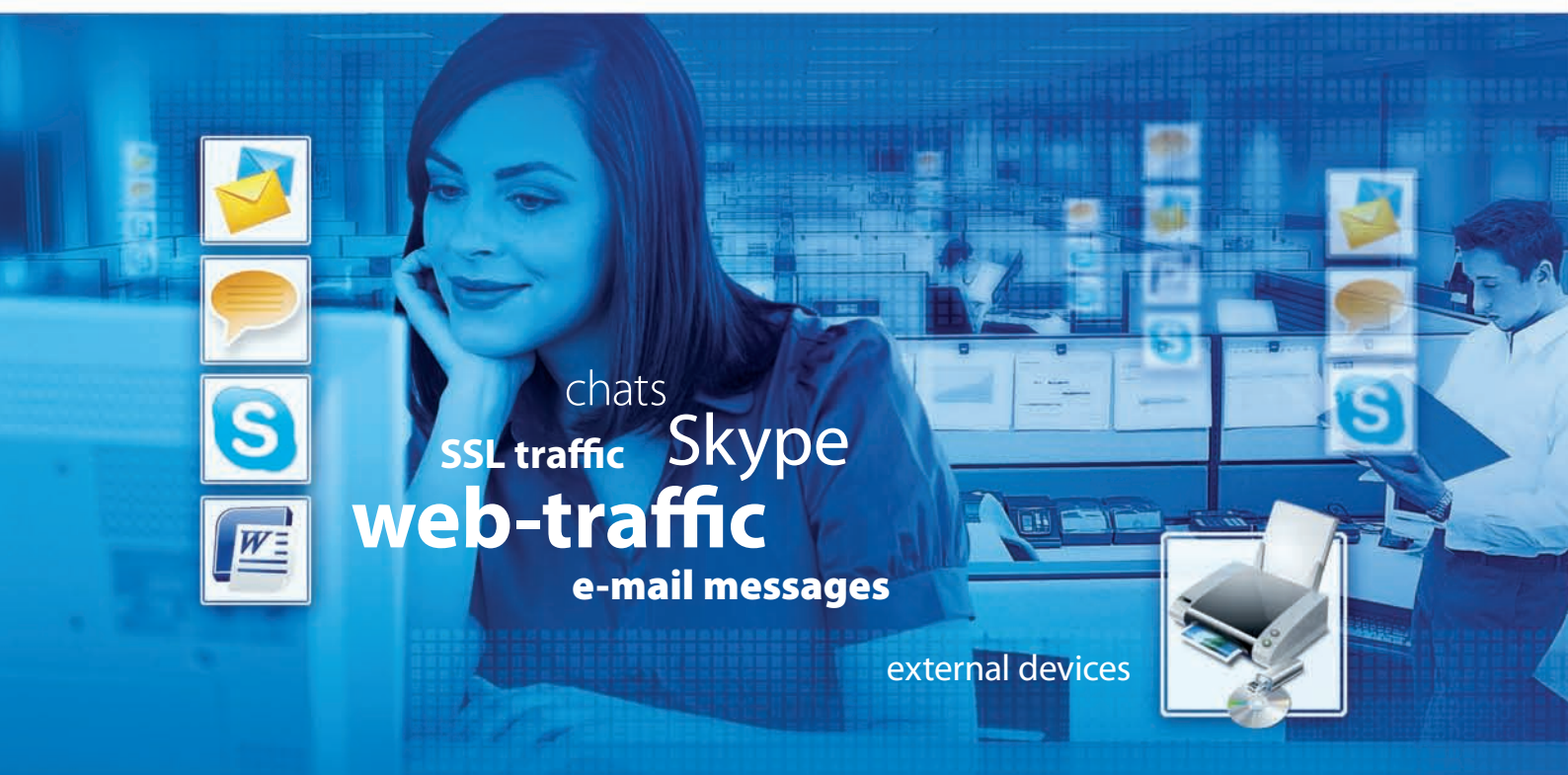
Protect your business from internal threats with SecureTower – a complex Data Leak Protection system

# Protect the core of your business

**SecureTower** is a complex solution designed for data loss protection and monitoring employees' network activities.

**SecureTower** is a compound system that is easily integrated into a corporate network and provides:

- Total control over possible data leaks through multiple channels;
- Users' network activities tracking;
- Assessing the efficiency of corporate resource usage by the employees;
- Creation of a unified archive of corporate communications.



**SecureTower** is a software solution that provides data leakage control over the following channels:

- **e-mail messages** created in POP3, SMTP, and IMAP protocols mail clients (i.e., MS Outlook, Thunderbird, The Bat!), MS Exchange Server mail;
- entire **web-traffic**, including e-mail messages of external mail clients (such as gmail.com), forum messages and posts, viewed pages of social networks and other web-services using HTTP protocol;
- **chats** and **conversations** in instant messengers using OSCAR (ICQ/AIM), MSN (Windows Live Messenger), XMPP/Jabber (Miranda, Google Talk, PSI) and other IM protocols, including Skype messages and voice calls;
- FTP, HTTP and HTTPS protocols' **files** transmission, IM-programs' file exchange (Skype, ICQ, Windows Live Messenger, etc.) and mail attachments;
- **SSL traffic** transmitted over encrypted protocols (HTTPS, encrypted ICQ and e-mail, etc.);
- data transferred to **external devices** (USB and storage devices, removable HDD, memory sticks, CD/DVD and floppy disks);
- data **printout** on local and network printers.

# Stay updated about all communications

## Monitor network activity

**SecureTower** creates comprehensive statistical reports on employee's network activities with the help of charts and diagrams, thus enabling you to see the way your corporate resources are used and estimate your employees' efficiency. **SecureTower** provides you with detailed description of sensitive data breach incident stating when, who and which network computer participated in it.

Visualization of employees' activities allows drawing side-by-side comparison of any employees' activity indexes, set for a definite time period.

Using our product, company's management or security department seeking to know how certain employees use network resources and work time, can keep track of each employee's network activities. The obtained results help assess employees' workload during the day, as well as efficient use of corporate resources. For instance, you can easily estimate the amount of working time spent on inappropriate activities not connected with direct job responsibilities (such as private talks and chatting in instant messengers, visiting work-unrelated web-sites, etc.).

## SecureTower as an HR tool

**SecureTower** can be used not only by security departments, but also by human resources specialists.

Graphic analyzer of all employees' communications helps to reveal most active network users, control their interaction with competitors and conduct personnel screening.

Thus, **SecureTower** can be an essential tool for HR department, as it facilitates staffing strategies of an organization and helps establish sound personnel management system.

## Unified communications' archive

Large companies prefer to keep all communications, both internal and external, in writing. In case some information discussed by employees and their management or a customer appears to be lost, misunderstood or simply forgotten, written communications help to easily and quickly find the necessary information or restore some past events.

All intercepted traffic is analyzed and stored in a database, thus helping to keep corporate business communications archive and investigate data leakage incidents in retrospective. Complete users' message history is available after selecting a certain message.



# Achieve ultimate security

## Rich functionality for data control

**SecureTower** monitors data leaks by analyzing all traffic on the basis of predefined context, attribute and statistical rules, taking morphology into account. The system provides detailed information about the data sender and recipient, and full text of an intercepted document or message. Additional protection is guaranteed by using data control based on regular expressions and digital fingerprints of documents and databases.

## Flexible security policies

**SecureTower** controls data leakage by analyzing traffic according to predetermined security rules. In case of a security breach **SecureTower** sends auto-alert to the e-mail address of the information security officer.

Consequently, security department gets automated notifications about all cases of unauthorized transmission of sensitive information even if it was sent with the help of encrypted channels or SSL protocols.

## Immediate user identification

Do your employees use terminal servers to connect to the network? We have a perfect solution for you! **SecureTower** can work with endpoint stations connected via terminal servers. You can identify such users, intercept and automatically analyze all their traffic. Basically, it does not matter to **SecureTower** whether it is a regular network or a terminal server connection. All users will be controlled in the same way.

**SecureTower** enables accurate identifying the actual data sender thus minimizing work-hours spent on security breach incident's investigation.

## AD integration

When you first install a DLP product you need to train it to recognize all users of your network. With **SecureTower** it is as simple as it can be: all users from your Active Directory can be automatically imported into the user list. One click – and all new users you add to your AD will simultaneously appear in the **SecureTower** interface. This feature will be especially valuable for large companies with huge numbers of employees, thus facilitating security officers' work.

## Technical and hardware requirements\*:

**CPU:** Pentium® 2 GHz and above

**Network adapter:** 100 Mbit/1 Gbit

**RAM:** 2 Gb minimum (+ 0.5 Gb for every 100 of controlled endpoints)

**HDD:** 110 Mb of space available for program files and a minimum of 30% of intercepted traffic amount for search index files, 300 Mb for client applications

**Microsoft .Net Framework:** 4.0

**OS for server components:** Microsoft Windows Server 2003 / Server 2008 (x86 or x64)

**OS for client components:** Microsoft Windows XP/Vista / 7 / Server 2003 / /Server 2008 (x86 or x64)

**Supported DBMS:** Oracle, Microsoft SQL Server, SQLite and Postgre SQL.

\* System requirements are individual for each component and largely depend on the characteristics and traffic loads in the network.



# Why SecureTower



## Comprehensive control over classified and personal data leaks

All conversations are controlled: IMs, including Skype, incoming and outgoing e-mails and attachments thereto, MS Exchange Server mail, and data transferred to removable drives, CD/DVD drives and printers. Moreover, the contents of sensitive documents and databases often containing important contacts and personal data are also under control.



## SecureTower is a multi-component and easily scalable system

The system consists of several server components performing different tasks and comprising a unique tool to keep track of all data transferred, regardless of the size and topology of the network. Our product is equally effective in small and in extensively loaded huge networks. Even if your corporate net has a multilevel structure with numerous workstations and servers, **SecureTower** enables you to keep everything under your total control. The system is highly scalable to meet any requirements and fit any network.



## Centralized setup of all system components and work in a single user console

Considering the complexity of mission performed by the DLP system, it needs flexible setup options and capability to tailor system behavior to the needs of an individual organization. In other cases this would result in use of multiple sophisticated tools to tune the system and make working with the product a real challenge. After installing **SecureTower** you will realize its usability. All components are located in a single console, and you always have easy access to everything you need.



## Easy to install and integrate into existing network

No special experience is required to install the product. If you have installed any software in Windows environment previously, you can handle it! Subject to your network characteristics, you may choose to install all system components onto a single machine or divide them between several computers. No changes are required to be applied to your existing network: **SecureTower** can work with whatever it sees in it.

## User-friendly interface

All information you have had so far about DLP solutions can make you think it is too difficult to operate this kind of software – there are so many things to tune and control that your company would have to hire another specialist or spend money to train the existing employees to use it effectively. However, take your time and think again – what if a DLP system is as easy to tune as a regular application, what if it has a self-explanatory interface? Can you imagine such a kind of DLP product? **SecureTower** is already there! It has a user-friendly interface, which means it can be used by anyone who is familiar with Windows OS and security requirements of your organization. At the same time, simplicity does not mean weakness to us. The system stays highly customizable and provides advanced control options.

## Improving security service efficiency

**SecureTower** minimizes time and cost of data leak incidents' investigation as it lowers percentage of false positives, thus raising the efficiency of security officers' work.

# About us

**FalconGaze** is a developer and supplier of complex high-performance premium-class data security products. The company provides compound solutions for continuous control over leaks and undesired disclosure of corporate sensitive information, tailored for monitoring workers' network activities.

The products we develop are not just regular software, but multi-component systems integrated into corporate networks. Our best practices and expertise in the sphere of information security are implemented in our products' development.

Our fundamental principles include individual approach and maximum customer's satisfaction leading to customized solutions for each client. **FalconGaze** software users are provided with a wide range of additional services that guarantee safe and reliable operation of our product. Our customers can be confident they are supplied with solutions that meet all modern information security requirements and ensure maximum data protection against insider threats.

We value our every customer and are ready to provide solutions that satisfy individual demands both of small and midsize businesses and of large corporations. The range of our potential customers is wide – from smaller companies with moderate-sized networks to large enterprises with complicated network topologies.

Our current business priorities include minimization of data leak and industrial espionage threats, as well as control of proper use of work time. With that, we are constantly diversifying the range of high-tech tools, we use to ensure our clients' data security.



## Contacts:

SoftMail Inc.



No. 1204, Mario-Tower,  
222-12 Guro-Dong, Guro-Gu, Seoul

Phone: +82 2 3486 9220

Fax: +82 2 3486 9331

[www.softmail.co.kr](http://www.softmail.co.kr)