

EFFICIENT PROTECTION
FROM INTERNAL THREATS

falcongaze
SecureTowerTM

Why SecureTower?

- Protects business from valuable data leakage
- Helps to reveal fraud schemes
- Controls efficiency of employees' work
- Captures suspicious activity
- Blocks malicious users' actions

SecureTower capabilities

- Control of data transmission channels
- Data analysis according to specified security policies
- Personnel loyalty evaluation
- Incident prioritization and investigation
- Wide capabilities for reporting

Software allows to combine different rules while security policies creating. It minimizes quantity of false alerts and increases efficiency of security service.

SecureTower Usage

Where is it used?

- In local networks of enterprise
- In networks with complex architecture
- In geographically distributed offices
- On mobile workplaces

Advantages

- Access control system
- Minimum load on workstations
- Easy integration with other security systems

Technical and system requirements*

SecureTower Server

Trial version (control of 25 working stations)

Processor: 2,2+ GHz (4 cores and more)

Network adapters: 1Gb

RAM: 6 GB and more

Hard disk: 100 GB partition for the OS and SecureTower files;
50 GB - for intercepted data storing (25 users per 1 month)

Operating system for server components:

Microsoft Windows Server 2008/2012/2016/2019 x64

Supported DBMS:

Microsoft SQL Server, Oracle, PostgreSQL, SQLite and MySQL.

Agent

The client's part on the controlled user's PC

The hardware configuration must comply with the Microsoft recommendations for the installed version of the operating system.

The operating system for agent:

Microsoft Windows XP/Vista/7/8/10/
Server 2003/ Server 2008/ Server 2012/ Server 2016 /
Server 2019

* The average estimated data are given. The system requirements depend on specific workstation control settings and storage period of intercepted data.

Incidents investigation

SecureTower provides opportunity to investigate security incidents. By adding new investigation, security officer can record in detail the progress of particular case and specify violators. Besides, when investigation is completed software automatically generates reports for CEOs. Collected data and reports can be considered as evidence by the court.



Risk analysis

This module analyzes each employee's activity according to configured rules and forms TOP-list by chosen criteria. It automatically generates reports for researching users' behavior tendencies. Module allows security specialists to evaluate current risk and take appropriate actions for security incidents prevention.

- Transliteration and fuzzy search
- Regular expressions
- Digital fingerprints
- Search by hash-functions
- Statistical analysis

Analytical capabilities

- Content analysis
- Analysis by thesauruses
- Detection of changed file-types
- Voice recognition
- Image recognition
- Stamps recognition
- CAD-files control



Visual reports

User activity

User activity control motivates personnel to take on more responsibility. Executives get full image of employee' working day: active and idle time, used applications and efficiency of work, as well as time spent on different web sites.

Interactive reports

This option grants analysis of business processes in the company and timely identify risky moments. Reports based on set criteria help evaluate work of specific employees and departments. All reports are interactive and allow shifting directly to the event review. Thus, the incident investigation process is significantly accelerated.

Graph-analyzer of personnel interactions

It tracks all employees' contacts both within and out of the company, including communication with competitors. Such a tool allows determining employees' social circle, identifying informal leaders and potential insiders, if data leakage is initiated outside.

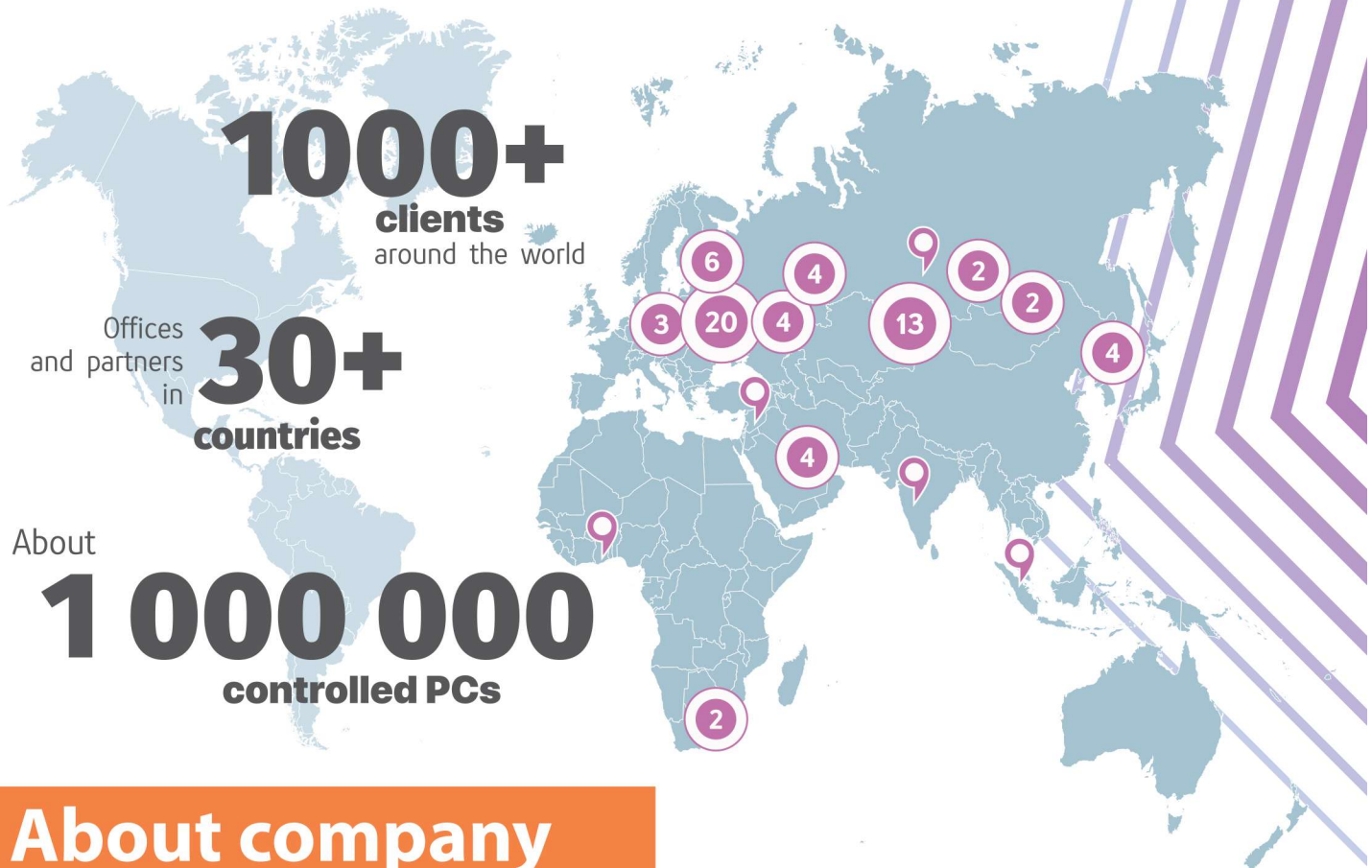
Working day pattern, video, and audio recording

SecureTower provides full working day pattern of each employee. Executives can evaluate efficiency of communication channel usage. Besides, user of SecureTower can connect remotely to employee's web-camera and desktop. Furthermore, audio and video recording is available for investigation process and employee's activity monitoring.

Control of communication channels

- E-mails
- Messengers
- Web-traffic
- Cloud storages
- Network-attached storages
- USB-devices
- Network and local printers
- IP telephony
- Workstations
- Clipboard





About company

Texode Company was founded in 2007. We develop and distribute high-tech premium-class product in the field of information security. Our comprehensive solution controls data leakage and unwanted spreading of commercial information. Besides, it grants employees' activity monitoring.

Contact us
to order trial
version or to
join us as
a partner

Texode LLC

Tel. /Fax: +375(17)385-24-50

Belarus, Minsk, 220114, Nezavisimosti ave., 117a, office 2

General information: contact@falcongaze.com

Sales department: sales@falcongaze.com

Technical support: support@falcongaze.com

Media contacts: pr@falcongaze.com