

Falcongaze SecureTower:

Workflows control and protection against insider threats



Falcongaze is a vendor of unconventional DLP-system SecureTower – comprehensive information security and user activity monitoring platform.

- **Firm foothold on domestic and traditional information security markets - within TOP 3 information security solutions in Russia**
- **Founded in 2007 and gradually growing ever since**
- **Widest distribution of customers from various industries and over 500 exclusive projects for most trusted companies and institutions in Russia and neighboring countries**
- **Dynamically expanding business to new regions with current presence in Eastern Europe, Asia and Africa**
- **Customer-centric operation model with “always-in-touch” attitude**

SecureTower is a multifunctional software solution for protection of a company against leaks of confidential data caused by carelessness or intentional acts of employees.

SecureTower is unconventional DLP system, which means comprehensive control of all data transmission channels + user activity monitoring + archive of all business communications.

Features:

- **Ultimate control over communication channels**
Detection, investigation and prevention of incidents
- **Deep insight into user activity at an endpoint and in the network**
All intercepted data are presented in an interactive and demonstrative form
- **Immediate access to any intercepted data**
Advanced search tool with diverse attributes and custom configuration options
- **Proactive search of irregularities and suspicious activity**

Retrospective analysis, graphical representation of workflow activities, analysis of user communications with colleagues and external contacts

Most information security experts agree: insider attacks always come unexpected and cause most painful impact on any company simply because insiders know exactly what they want and where it is.

Conventional information security and data leak prevention practices have already failed these companies:



Korea Credit Bureau



Barclays Bank



DuPont



EnerVest



AT&T

All of them were compromised by employees or contractors in 2014, bearing multi-million dollar losses and inestimable reputation damage.

With new and effective technologies for protection from intrusions and external attacks, insider threats are gaining more prominence than ever before.

No one wants to become a part of statistics.

How SecureTower manages insider threats



Control of information flows and data leak prevention



Control of performance and effectiveness of business processes



Monitoring loyalty of employees



Archiving all business communications

Controlled data transfer channels

E-mail

Mail servers

Social networks

Visited sites

**Instant
messaging**

**External
devices**

Printers

Clipboard

IP-telephony

Sent files

Keylogger

Network shares

**Recording from
microphone**

**Application
control**

Screenshots

**Control
of work hours**



Endpoint agents

- **Mail** (SMTP(S); POP3(S); MAPI (non-encrypted);
- **WEB control**: HTTP(S)
- **Messenger control** (including encrypted)
- **External devices and peripherals**
- **FTP(S)**
- **Comprehensive user activity control**



SPAN-port

- **MAIL control**: SMTP, POP3, IMAP, MAPI
- **WEB control**: HTTP
- **Messengers control** (non-encrypted)
- **FTP**



Mail processing server

- **MS Exchange (EWS)** and other systems which use **POP3** and **SMTP** protocols (Lotus Domino, Kerio Connect, Postfix, Sendmail and others).



ICAP-server

- **WEB control**: HTTP(S)



Office personnel



Road warriors



External contacts



Cloud storages



**Network shares
& peripherals**

System requirements

- **CPU:** 2,4 GHz
- **Network adapter:** 1 GBit
- **RAM:** 8 GB and above
- **HDD:** 300 MB for program files and about 3% of intercepted traffic for search index files
- **Microsoft .Net Framework 4.0**
- **OS for server components:** Microsoft Windows Server 2003/2008 x64
- **OS for client components:** Microsoft Windows XP/Vista/7/8/Server 2003/Server 2008/Server 2012 (x86 или x64)
- **Supported DBMS:** PostgreSQL, Microsoft SQL Server, Oracle, MySQL, SQLite

Collected data

- 1200 MB per user per month (full functionality)

Agent-Server

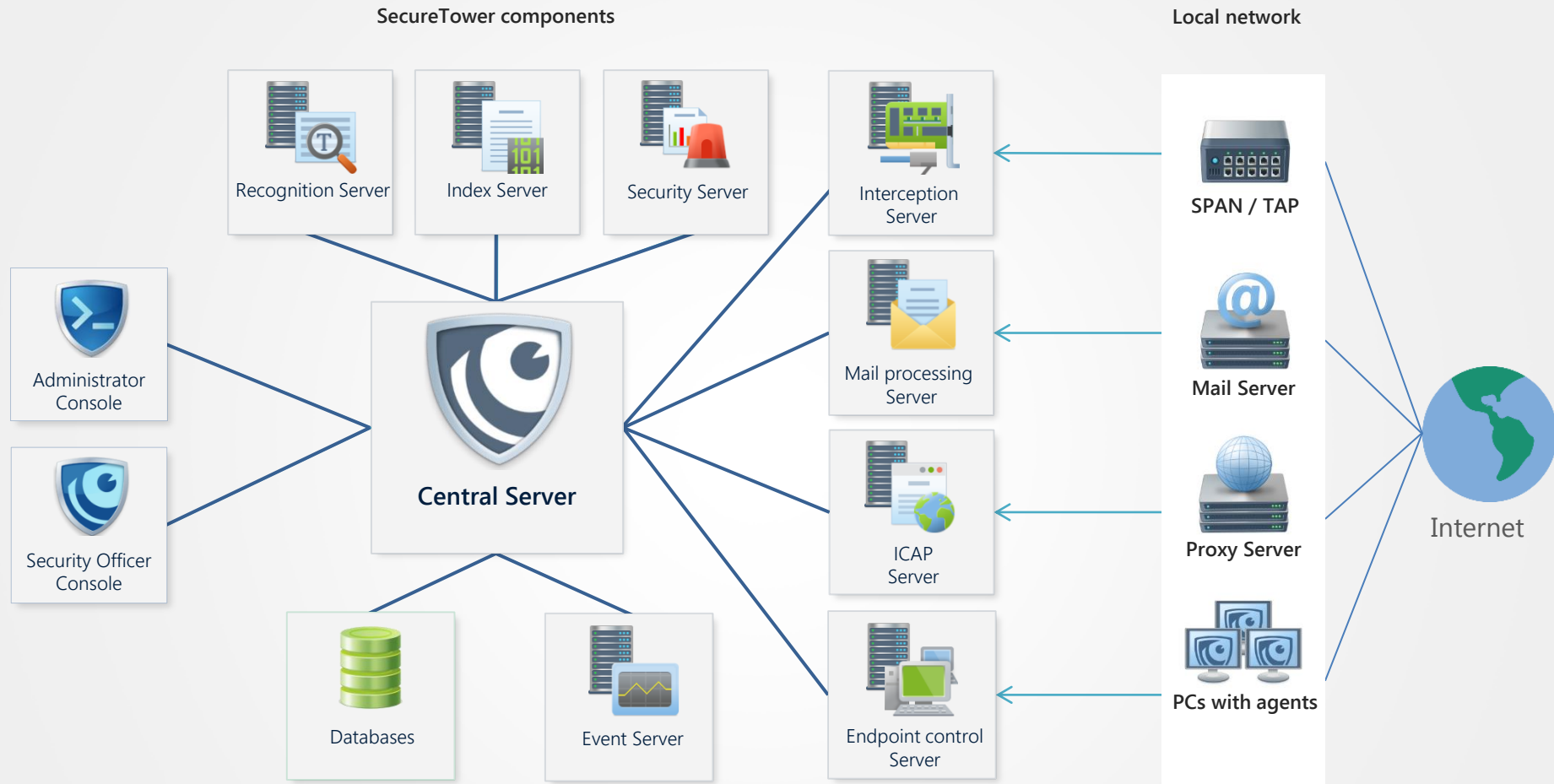
- Connection once a minute. Immediate data transfer on interception of 8Mb and more

Bandwidth impact

- Configurable data transfer speed for low performance networks

Scalability

- Unlimited (SecureTower is 100% software with modular structure)





**Information
Security
Officers**



**Business
owners**



**Top
management**



HR specialists



**Small and medium
business**

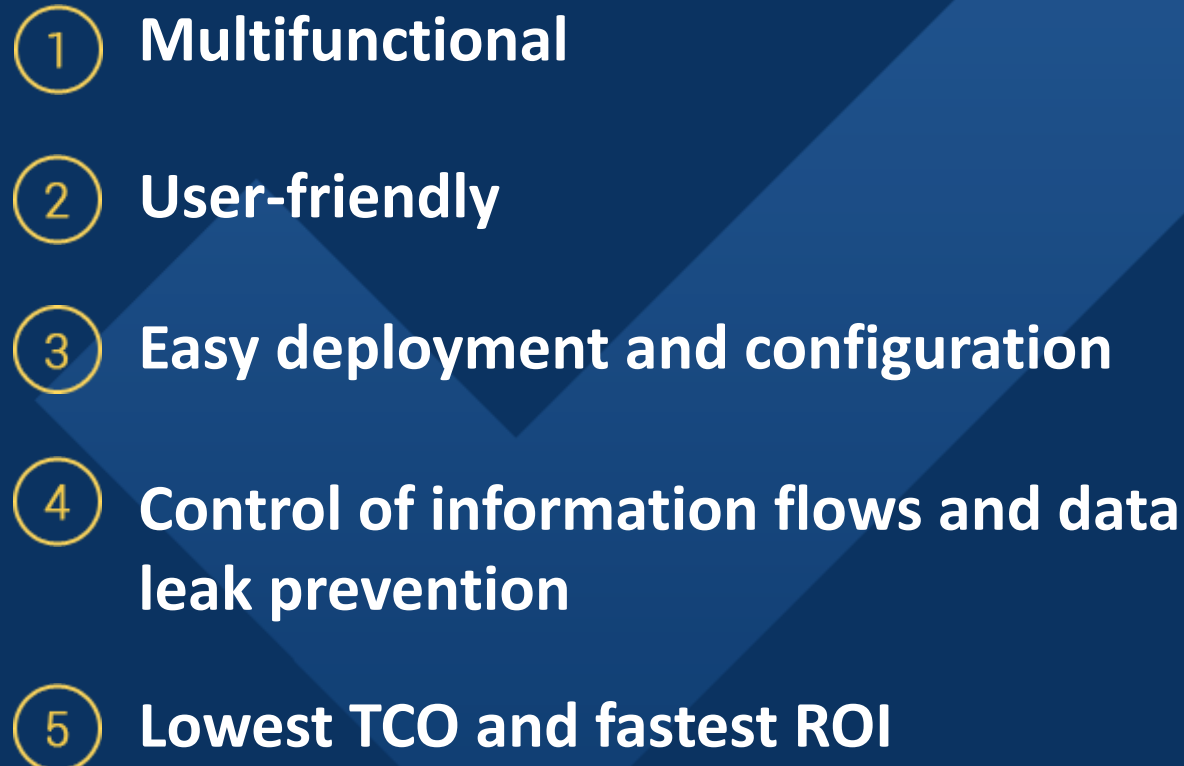


Big corporations

Got sensitive data, classified information, PII/PFI or commercial secrets?

Most of our customers come from the following industries:

- **Financial sector (banks and insurance companies)**
- **Energy sector**
- **Broadcasting and telecom**
- **Public sector**
- **Carriers, transport and logistics**
- **Industrial enterprises**
- **Retail sector and trade companies**
- **R&D and innovations**
- **Healthcare**





- 
- ① **Multifunctional**
 - ② **User-friendly**
 - ③ **Easy deployment and configuration**
 - ④ **Control of information flows and data leak prevention**
 - ⑤ **Lowest TCO and fastest ROI**

- ⑥ **Economic security and control of corporate resources**
- ⑦ **Smart user monitoring tool**
- ⑧ **Vivid and interactive reporting**
- ⑨ **Control of all major data transfer protocols**
- ⑩ **Archiving all business communications**

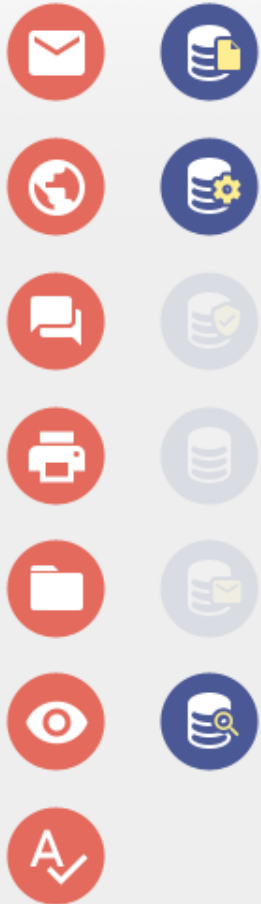
Modules

-  **M1. Corporate mail**
-  **M2. External mail and web resources**
-  **M3. Messengers**
-  **M4. External devices**
-  **M5. FTP(S)**
-  **M6. User activity monitoring**
-  **M7. Image recognition**

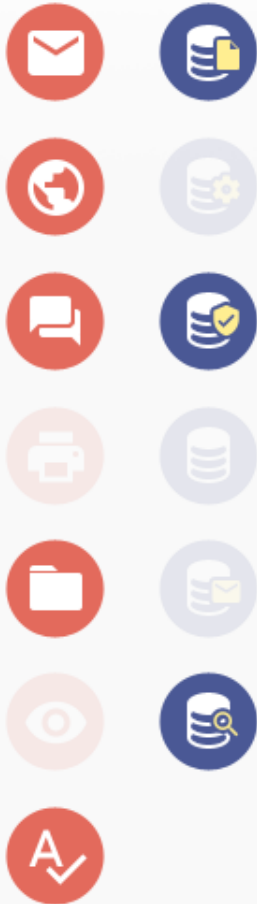
Server components

-  **S1. Data processing server**
-  **S2. Endpoint agent control server**
-  **S3. Interception server**
-  **S4. ICAP server**
-  **S5. Mail processing server**
-  **S6. Image recognition server**

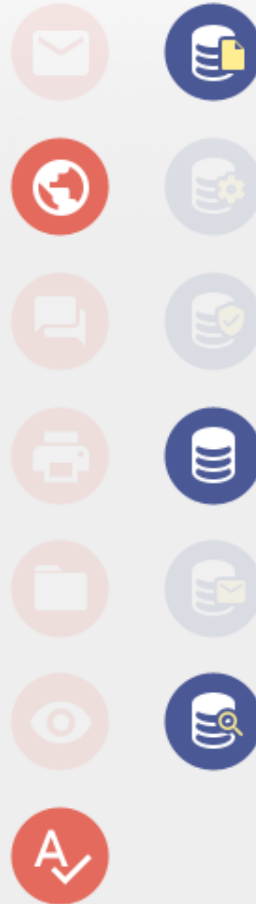
Interception with Endpoint agents



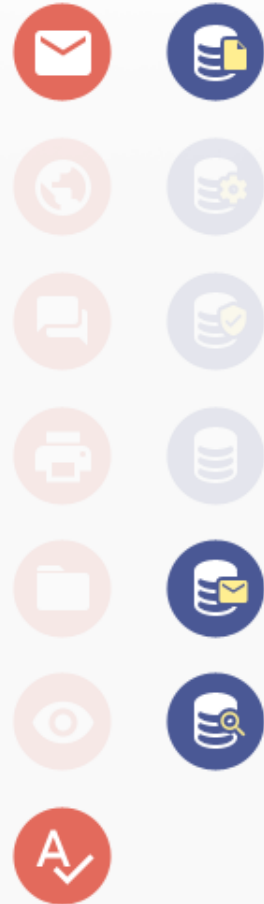
Interception with SPAN-port



Interception with ICAP-server



Interception with Mail processing server



Licensing is based on the number of users/machines (N) and number of server modules:



Endpoint agent interception = N of users + Endpoint agent control server + Data processing server;



SPAN-port interception = N of users + Data interception server + Data processing server;



Combined interception = N of users (agent scheme) + Endpoint agent control server + Data interception server + Data processing server;



Mail processing server interception = number of mailboxes + Data processing server + Mail processing server



ICAP server interception = N of users + Data interception server + ICAP server

SecureTower licensing models

Perpetual

YOU BUY – YOU OWN policy:

- Reasonable and highly competitive cost of the Product;
- Once purchased SecureTower will be fully operational for unlimited time;
- We charge only maintenance, updates and technical support at only 25% of the cost annually (first year is free);
- Maintenance, updates and technical support payments are **NOT** mandatory;
- Welcoming “come-back policy” for renewal of maintenance, updates and technical support contract.

Subscription

RENT-A-SOFT policy:

- Most affordable prices;
- Clear and Convenient annual payments;
- Use SecureTower only when you need, save money when you don't and welcome back again soon!
- Get all benefits of full functionality for less.

Thank you

Contact us or our regional partners for all inquiries
See more on www.Falcongaze.com

Email: sales@PanzerIT.com | Website: www.PanzerIT.com

Ph: +91 22 4974 4416 | +91 90046 55099

902, Vashi Infotech Park, Plot No 16, Sector 30A, Vashi, Navi Mumbai 400 705