



## StaffCop Enterprise

**MONITOR. ANALYSE. REPORT. BLOCK**

A bundled software solution to control information, user actions and system events on workstations

For business and government organizations with 5 to 25 000+ employees

[staffcop-enterprise.com](http://staffcop-enterprise.com)





# STAFFCOP

## MONITOR. ANALYSE. REPORT. BLOCK

dangerous and unproductive user activity

For business and government organizations  
with 5 to 25 000+ employees

A bundled software solution to control information, user actions and system events on workstations



### Threat detection at an early stage

The information security system features flexible configuration of filters and alerts, thus helping to prevent data leak at an early stage and considerably reduce negative consequences.



### Working time tracking

Track user activity on workstations. Track working time, lateness, days out and down time.



### Employee efficiency evaluation

Categorize applications and web-sites into productive and unproductive. Set up different configurations for particular users, groups and departments. Compare results.



### Monitor business processes

Detect "bottlenecks", blocking factors and investigate the reasons of their cause KPI-based analysis of business-processes.



### Investigate incidents

StaffCop is a time machine! At any moment you can go back in time and see what a particular employee was doing in the specified period of time.



### User Behavior Analytics

Analyze anomalies in user behavior. Handy means of visualization statistical information: heat map, graph and relation tree.



### Live administration

View remote desktop without being noticed. Take control over a workstation. This function is helpful for IT-specialists and information security officers.



### Workstations inventory

Full picture of software and hardware usage. Intensity of usage and registry of states.

## Handy and useful!



### Powerful analytics

Content files analysis, graphs and diagrams to visualize data, relation graphs, multi-dimensional reports.



### Handy web-interface

Monitor and manage the system from your favorite browser or any place with connection to the internet.



### Modern technologies

StaffCop is based on the OLAP-technology of data processing allowing to build multi-dimensional reports "on the fly" and process huge volumes of data within seconds.



# HOW STAFFCOP WORKS



StaffCop is a unique, fully-integrated solution to monitor employee activity, information channels and system events featuring advanced analytics system for detecting disloyal employees and prevention malicious actions.

- Helps to reduce risks of data leakage and loss of reputation
- Allows you to see your business processes in reality
- Provides transparency of work
- Quick investment return & minimum maintenance cost
- Handy web-interface
- Easy deployment

## Staffcop Enterprise is based on client-server architecture

Agents and administrators connect to the server via encrypted HTTPS protocol. Any types of infrastructure are supported, including NAT-translation, VPN-channels and other variants of connections. This gives the possibility to operate on a remote computer which is not located in the local network of a company.

## Offline mode – monitor users even when they are unavailable

If an agent can't connect to the server, it stores data in its local database and starts transferring it to the server at the first opportunity. This function allows to carry out constant monitoring of employees connecting to the internet using temporary channels – mobile 3G/4G modems, public Wi-Fi networks, e. t. c. So, in case an employee goes on a business trip with his working laptop, he keeps being monitored and controlled. Staffcop Enterprise requires only one server running GNU/Linux-based OS to collect, store and analyze data on user activity.

## StaffCop Enterprise consists of two parts: server module and endpoint.

An endpoint agent is launched on a workstation or terminal server running Windows or Linux, collects data on user activity and transfers it to the central server to be processed and visualized.

### Collect

Collect all activity events on endpoints for following analysis, notifications and decision making.

### Analyze

Automatic and statistical analysis of data to detect anomalies of user behavior, identify incidents, insiders and disloyal employees.

### Alert

Automatic alerts on violations of security policies, dangerous and unproductive activities of employees.

### Report

Pre-configured & self-made reports with periodic e-mail sending. You can easily create reports with a powerful constructor.

### Block

Locking access to forbidden sites, applications and removable USB-storages to reduce the risk of malware infection and increase employee productivity.

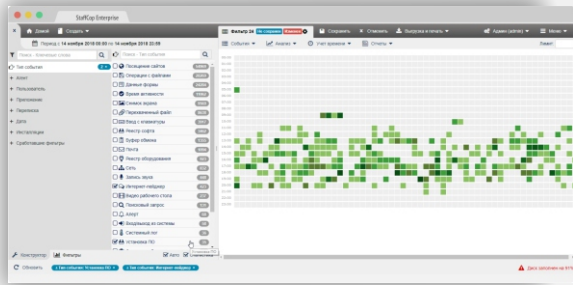
### Investigate

Search all data using keywords and regular expressions, easy correlation & drilldown allows you to find data cleared from noise in a few clicks.

# INFORMATION SECURITY



StaffCop is based on modern technologies of data interception and analysis



## POWERFUL ANALYTICS

- Hash-based document search
- Content analysis of documents
- Text search by regular expressions
- Embedded OCR module (text recognition in images)
- Automatic detector of behavior anomalies
- Built-in and custom dictionaries
- Detection of encrypted archives
- Multi-dimensional interactive reports
- Relation graphs
- Heat maps
- Analytical tables and graphs

## ALERTS ON THREATS

Staffcop can send alert about violations of security policies in the administrative panel or to e-mail.

Using the Constructor you can easily create various policies with corresponding to the security policies of your company and set up alerts when filters are triggered.



[staffcop-enterprise.com](http://staffcop-enterprise.com)

## INTERCEPTION OF ALL CHANNELS AND EVENTS

on workstations and terminal servers

### Email protocols

IMAP, SMTP, MAPI, POP3 and their encrypted analogues. Control of sending messages and files from e-mail web-services.

### Instant Messengers

Skype, ICQ, Jabber (XMPP), MSN and other. Using the relation chain 'key-logger – application/site – screenshot' one can track communication via any messengers, chats or other web means of communication.

### Applications

Facts of installations and launching of events, duration of usage, screenshots made when changing active window. Lock launching of processes and applications.

### Files

Log all file operations, including operations with network directories. Shadow copying of files sent outside the local network of a company.

### USB ports

Monitor operation with removable storage. Lock USB-devices by classes and HWID. Switch USB and CD to read-only mode.

### Printing

Log printing events: user, time, computer, number of printed pages e.t.c. Shadow copying of printed documents.

### Network activity

Log network connections and control encrypted web-traffic, monitor web-sites visiting and search queries.

### SIP

Log calls and their duration, intercept SMS.

### Audio and video record

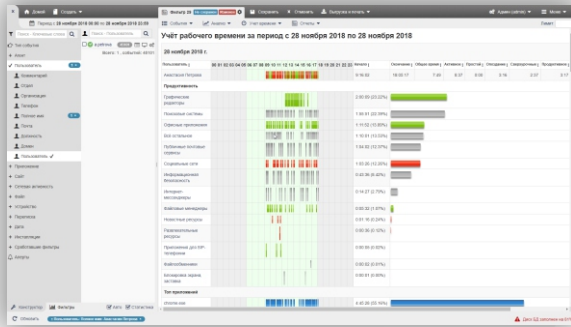
Record sound from microphones, desktop video, desktop screenshots and web-cam snapshots.

# INVESTIGATE INCIDENTS



## StaffCop is a time machine!

At any moment you can go back in time and see what a particular employee was doing in the specified period of time.



You can receive the required data “on the fly” using the Constructor of multi-dimensional reports. Search by keywords and regular expressions helps to reduce the time of incident investigation to minimum and the ability to record sound from microphones allows to hear what was happening at the moment of interest.

## Relation graphs

Visualization of communication between employees and its intensity. Schema of files migration within and beyond the local network of the company.

## Anomalies detection graphs

Linear graphs, pie charts, histograms and analytical tables. They help to visualize data in a convenient way.

## Heat map

Visualize intensity of user activity and events.

## Dimension cards

Summary reports displaying characteristics of an object and related events. Card of an employee, file, site, e.t.c.

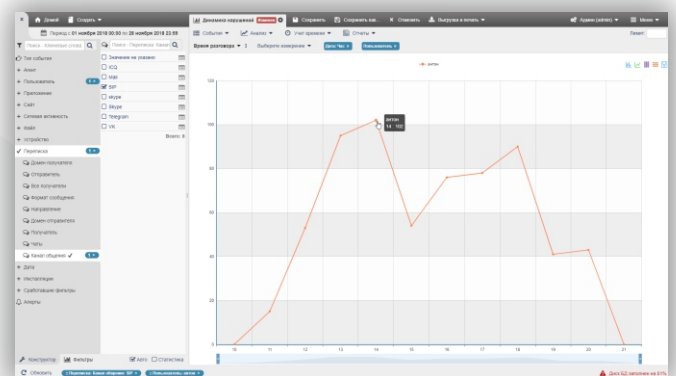
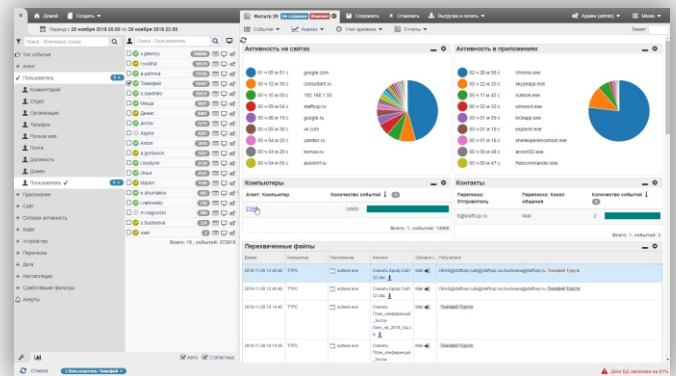
## Data export and printing

Reports and events can be exported to PDF or Excel.

## Fast! Even with big data

OLAP-cube model makes data analysis extremely flexible: building chains at incident investigation, fast switch from general to specific, building analytical reports on the chosen slices of data.

Combined usage of PostgreSQL and ClickHouse extremely increases the speed of processing data. You don't have to set up reports to be generated over the night to learn that there's nothing useful there – now you can investigate in real time!



Запись звука

Запись с микрофона Вести запись с обнаруженных микрофонов.

Запись звука колонки Вести запись звука колонок.

Длительность прерывания, секунды: 600 Вести запись прерывания указанной длительности.

Уровень записи, от 0 до 100: 80 Уровень записи в процентах от 0 до 100. Для использования уровня, уже установленного на компьютере, введите 0.

Интервал тайминга: 5 Если нет звуков в течение указанного интервала, то запись прерывается.

Качество записи: 0 При менее 0 - меньше размер, при более 0 - лучше качество.

Шумовой порог, от 100 до 190: 0,0 Игнорировать звуки при уровне сигнала ниже заданного.

# EMPLOYEE MONITORING ON GNU/LINUX



StaffCop works on modern distributives including Ubuntu, Debian, Red Hat and Arch Linux.

Monitor and analyze user actions on workstations with X-Windows window manager as well as in terminal mode.

## System log in/out

StaffCop registers every event of user log in and log out of the system, including users connected remotely and using SSH.

## Screenshots

StaffCop takes screenshots at a specified time interval and changing the active window

## File operations

StaffCop logs file operations: read, write, remove, create and rename. Shadow copying.

## Activity time in applications

StaffCop logs all user activity time in applications. Collected data is used to build employee productivity report. Report data corresponds with screenshots with the help of time tags. Fast drill-down from graphs and tables to events.

## Key-logger and bash-logger

Staffcop intercepts key-strokes at the kernel level to control server terminals and keyboard input in X-sessions.

## Record sound

Record sound from built-in and connected microphones. You can configure the noise threshold, lengths of recorded fragments and the level.

## Monitor USB-devices

Flash drives, printers or other peripherals are logged. Administrator can get information on connection of devices including the time and the target workstations.

## Monitor web-site visiting

StaffCop logs all site visiting in Chrome, Firefox and browsers based on their engines. The amount of time users spent on particular web-sites is tracked.

## Monitor document printing

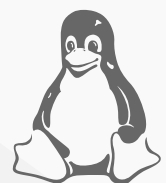
Printing events are logged, with such details as user name and file title.

## Monitor log-files

StaffCop Enterprise tracks changes in the log files including syslog. Every change of a log file is considered a separate event.

## Clipboard

StaffCop intercepts the content of the clipboard. Administrator views intercepted data and sorts them using various filters.



# WORK TIME TRACKING



StaffCop logs not only the beginning, the end of the working day and the breaks but displays detailed picture of each employee working day.

Unique algorithms of activity recognition allow precise time tracking for applications and web-sites.

## Time tracking for period from 1 June 2018 to 30 June 2018

June 1, 2018																																			
Account	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Start of work	End of work	Total time	Active	Down time	Lateness	Overtime	Productive	Unproductive	Neutral	
Anton																									12:13:34	18:57:13	6h 43m 39s	10h 03m 27s		00s	5h 43m 34s	3h 59m 05s	10h 02m 04s	23s	01m 18s
Aspire																									11:15:27	19:46:54	8h 31m 27s	10h 39m 19s		00s	4h 45m 27s	3h 35m 20s	8h 04m 49s	00s	2h 34m 57s
driver																									8:30:34	11:42:12	3h 11m 38s	31m 47s	2h 39m 51s	2h 34s	00s	30m 30s	00s	01m 20s	

## Lateness report from 1 June 2018 to 30 June 2018

The ratio of the total time to the total time delays		Number
Total time	539h 45m	
Total time delays	205h 24m	

Top latecomers	Number
Maxim	17
Anton	17
roman	5

Top time delays	Number
Anton	80h 24m
Maxim	85h 31m
roman	30h 28m

Account	Number of lateness	Total time delays	Total time	Active time	Downtime
Anton	17	69h 24m	162h 17m	217h 20m	6h 10m
roman	5	30h 28m	25h 04m	12h 15m	12h 49m
Maxim	17	85h 31m	152h 23m	153h 14m	20h 22m
Total	39	205h 24m	339h 48m	382h 56m	39h 22m

## Visualized statistics:

- Lateness
- Downtime
- Active time
- Productive
- Time spent on personal needs
- Statistics by employees and departments

Employee productivity increases in average by 38% after StaffCop deployment.

## Scheduled e-mail reports

StaffCop can send daily colorful PDF reports to your e-mail.



It's almost as good as morning newspaper, but instead of canards and gossips you will get verified facts.

## Work schedule for departments and particular employees

Not all employees work from 9AM to 6PM, from Monday to Friday. Sometimes they take sick leaves or vacations.

In StaffCop you can setup work schedules taking into consideration all the peculiarities of employees' schedules.

This gives the ability to get precise information on lateness and overtimes and to receive summary information on departments.

июнь, 2018						
Понедельник	Вторник	Среда	Четверг	Пятница	Суббота	Воскресенье
28 Май 09:00 - 18:00	29 Май 09:00 - 18:00	30 Май 09:00 - 18:00	31 Май 09:00 - 18:00	1 Июнь Выходной	2 Июнь Выходной	3 Июнь Выходной
4 Июнь 09:00 - 18:00	5 Июнь 09:00 - 18:00	6 Июнь 09:00 - 18:00	7 Июнь 09:00 - 18:00	8 Июнь Выходной	9 Июнь Выходной	10 Июнь Выходной
11 Июнь 09:00 - 18:00	12 Июнь 09:00 - 18:00	13 Июнь 09:00 - 18:00	14 Июнь 09:00 - 18:00	15 Июнь Выходной	16 Июнь Выходной	17 Июнь Выходной
18 Июнь 09:00 - 18:00	19 Июнь 09:00 - 18:00	20 Июнь 09:00 - 18:00	21 Июнь 09:00 - 18:00	22 Июнь Выходной	23 Июнь Выходной	24 Июнь Выходной
25 Июнь 09:00 - 18:00	26 Июнь 09:00 - 18:00	27 Июнь 09:00 - 18:00	28 Июнь 09:00 - 18:00	29 Июнь Выходной	30 Июнь Выходной	1 Июль Выходной

# EMPLOYEE EFFICIENCY ANALYTICS



StaffCop reveals the amount of time spent by each user on work and personal needs.

You can setup different categorization of applications and web-sites for various groups of employees, specifying those required for work and those that shouldn't be used.

Time tracking for period from 1 June 2018 to 30 June 2018

Account	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Start of work	End of work	Total time	Active	Down time	Lateness	Overtime	
June 1, 2018																																
Anton																										12:13:34	18:57:13	6h 43m 39s	10h 03m 27s	00s	5h 43m 34s	3h 59m 05s
Irina																										10:53:49	18:22:22	7h 28m 33s	12h 19m 03s	00s	4h 23m 49s	3h 19m 03s
Matvey																										11:32:42	23:59:59	12h 27m 17s	11h 43m 42s	43m 35s	5h 02m 42s	4h 21m 27s
Maxim																										11:47:42	18:51:11	7h 03m 29s	9h 02m 40s	00s	5h 17m 42s	3h 18m 10s
oksana																										8:41:36	19:19:07	10h 37m 31s	12h 45m 25s	00s	2h 11m 36s	4h 07m 38s
roman																										15:59:32	16:05:44	06m 12s	01m 14s	04m 58s	9h 29m 32s	00s
Yuriy																										10:18:29	19:14:59	8h 56m 30s	11h 59m 47s	00s	3h 48m 29s	3h 35m 54s
June 2, 2018																																
Matvey																										0:00:06	23:53:31	23h 53m 25s	5h 54m 01s	17h 59m 24s	00s	5h 54m 01s
Maxim																										16:51:03	18:24:36	1h 33m 33s	54m 02s	39m 31s	00s	54m 02s
June 3, 2018																																
Matvey																										11:21:00	23:59:59	12h 38m 59s	8h 06m 18s	4h 32m 41s	00s	8h 06m 18s
June 4, 2018																																
Anton																										12:02:06	21:12:43	9h 10m 37s	8h 38m 20s	32m 17s	5h 32m 06s	2h 59m 29s

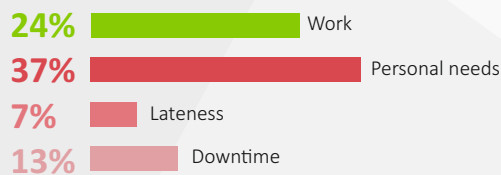
- Green bars – productive activity
- Red bars – unproductive or dangerous
- Grey bars – neutral activity
- No bars – no activity registered

## Lock distracting applications and web-sites.

Any site or application distracting an employee from his work can be locked for this particular employee, an entire department or for every user.

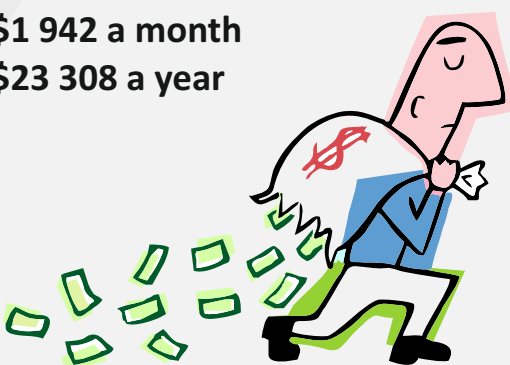
## In figures

We have reviewed about 200 companies using StaffCop with more than 4500 employee in summary, and made out a picture of a usual working day:



financial loss from unproductive activity and lateness of 10 employees with average salary of \$440 a month:

**\$1 942 a month**  
**\$23 308 a year**



## Summary reports by departments

Отдел "office"			
Приложение	Время	Сайты	Время
chrome.exe	09:28	staffcop.ru	06:56
outlook.exe	03:38	192.168.1.134	01:04
skype.exe	01:54	192.168.1.109	00:37
excel.exe	01:15		00:13
winword.exe	00:37	staffcop.ru	00:10
Отдел "marketing"			
Приложение	Время	Сайты	Время
chrome.exe	07:56	staffcop.ru	04:57
powerpnt.exe	04:36	google.ru	00:52
connect.exe	04:16	vk.com	00:23
skypeapp.exe	02:12	192.168.1.134	00:20
outlook.exe	01:15	yandex.ru	00:16

- Productive time by departments
- Unproductive top by departments
- Track presence at workplace
- Active time by departments

# LIVE ADMINISTRATION AND IT AUDIT



Monitor processes and applications, system events, and remote desktop connection makes StaffCop Enterprise a must-have tool for an IT specialist.

You can see who and when installed or uninstalled applications, control network connections, lock launch of prohibited applications and web-sites.

All data in one place,  
no more troubles with logs and proxy.

## Lock sites and applications

StaffCop gives the ability to set a whitelist of sites and applications for work, blacklist those distracting from work. Lists can differ for various users and groups.

## Monitor and control USB

StaffCop allows obtaining the list of all the applications installed on a workstation and the list of hardware with HWIDs. Log and lock USB-connections by device class. Monitor file operations and intercept files transferred to USB, read-only mode for removable drives.

## Remote desktop

StaffCop Enterprise gives you the ability to view all employee activity on online-mode and, in case of necessity, take control over a workstation, no passwords or authorization required.

## Software and hardware inventory

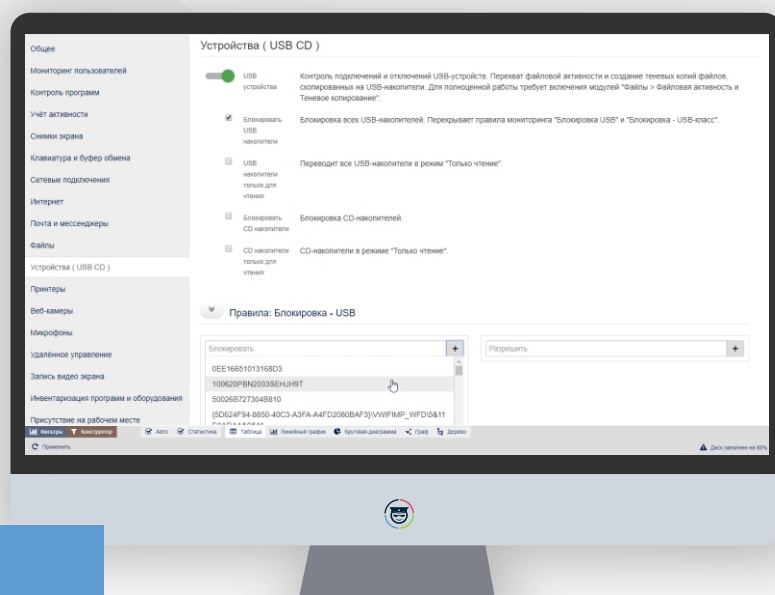
StaffCop collects information about the devices and applications installed on workstations. It gives the ability to detect if any hardware is lost or replaced and to detect installation of "prohibited" applications.

## Software installation control

StaffCop allows obtaining the list of all the applications installed on a workstation and the list of hardware with HWIDs.

## Network activity

Allows tracking IP addresses, ports and applications used for connection.



# STAFFCOP ARCHITECTURE



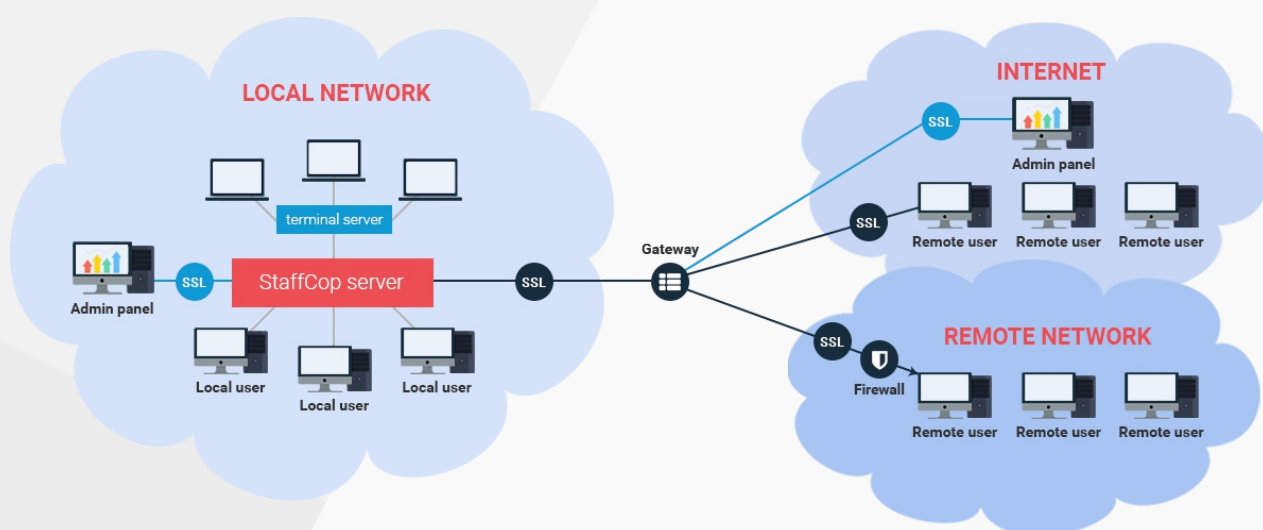
## Control workstations and terminal servers in local and distributed networks of any complexity.

Control network infrastructure, based on client-server architecture via VPN, NAT and other channels.

Monitor workstations  
in local networks

Centralized control  
over remote offices

Control remote employees



## ENDPOINT AGENTS

An endpoint agent is launched on a workstation or a terminal server running Windows or Linux, it tracks user activity and events on a workstation, transfers them to the server and employs various locking policies.

A Staffcop Enterprise agent can work on a remote computer which is not located in the local network of the company.

## SERVER

StaffCop Server works on Ubuntu Server 16.04 LTS amd64 and can be deployed on bare-metal, virtual machine or VDS/VPS server. StaffCop requires only one server to collect, analyze and view information on user activity and intercepted data.

### Supported OS

Windows:  
Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 10.1,  
Windows XP - limited functionality.

Terminal servers on Windows:  
Windows 2008, Windows 2008 R2,  
Windows 2012 R2, Windows 2016.

GNU/Linux:  
Ubuntu, Debian, CenOS, Gentoo, Arch, Rosa, AstraLinux.

### Can be deployed on Windows

For that you need to install VirtualBox environment and then install StaffCop Server on it.

### Supports visualization environments

WMWare, VirtualBox, Hyper-V и Proxmox

### PostgreSQL and ClickHouse hybrid mode

Using OLAP-technologies with these 2 databases increases speed of report building and system operation