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
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

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.

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.

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.com
StaffCop is based on modern technologies of data interception and analysis.

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.

POWERFUL ANYLITICS

- 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
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!

staffcop-enterprise.com
StaffCop works on modern distributives including Ubuntu, Debian, Red Hat and Arch Linux.

**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.
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.

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

**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.

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

**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.

staffcop-enterprise.com
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.

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:

- 24% Work
- 37% Personal needs
- 7% Lateness
- 13% Downtime

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

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

staffcop-enterprise.com
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.

**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-enterprise.com
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.

**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 XP - limited functionality.

Terminal servers on Windows:
Windows 2008, Windows 2008 R2,

GNU/Linux:
Ubuntu, Debian, CentOS, 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**
VMWare, 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