



INFOWATCH®

INFOWATCH TRAFFIC MONITOR



EMPLOYEES ABUSE DATA ACCESS RIGHTS

Many companies defend themselves from viruses and external attacks, while the biggest threat comes from within. Even ordinary employees have access to company's entire infrastructure: they send hundreds of emails, communicate in messengers and vent emotions in social media, upload data to file hosting and cloud storages, use corporate data on smartphones and tablets, and access business systems via virtual environments.

Such ample opportunities and access to any information from any device make employees a major threat to business integrity and security:



Fraud



Using corporate resources for personal purposes



Spying for competitors



Discrediting company by publishing sensitive information on the Internet



Selling customer bases on the black market



Stealing know-how, trade secrets, and other confidential data, thus causing business losses

InfoWatch Traffic Monitor is designed to address internal threats and staff misconduct, which cause business data leaks and financial losses



These circumstances require a new approach

- Protection of large data volumes of any format
- Data protection on various devices (smartphone, tablet, laptop, workstation, remote desktop)
- Data protection across various operating environments (business applications, corporate email and webmail, messengers, etc.)

KEEP YOUR DATA SECURED

① Discover

Detect suspicious events to reveal data leaks and employee misconduct

② Analyze

Use analysis tools to detect sensitive data in the flow of events, with category and topic being identified automatically

③ Make decisions

Respond according to your corporate policies (get alerts or block processes) and define severity of each threat

④ Keep evidence

Store all events in a single archive as an evidence base for incident investigations

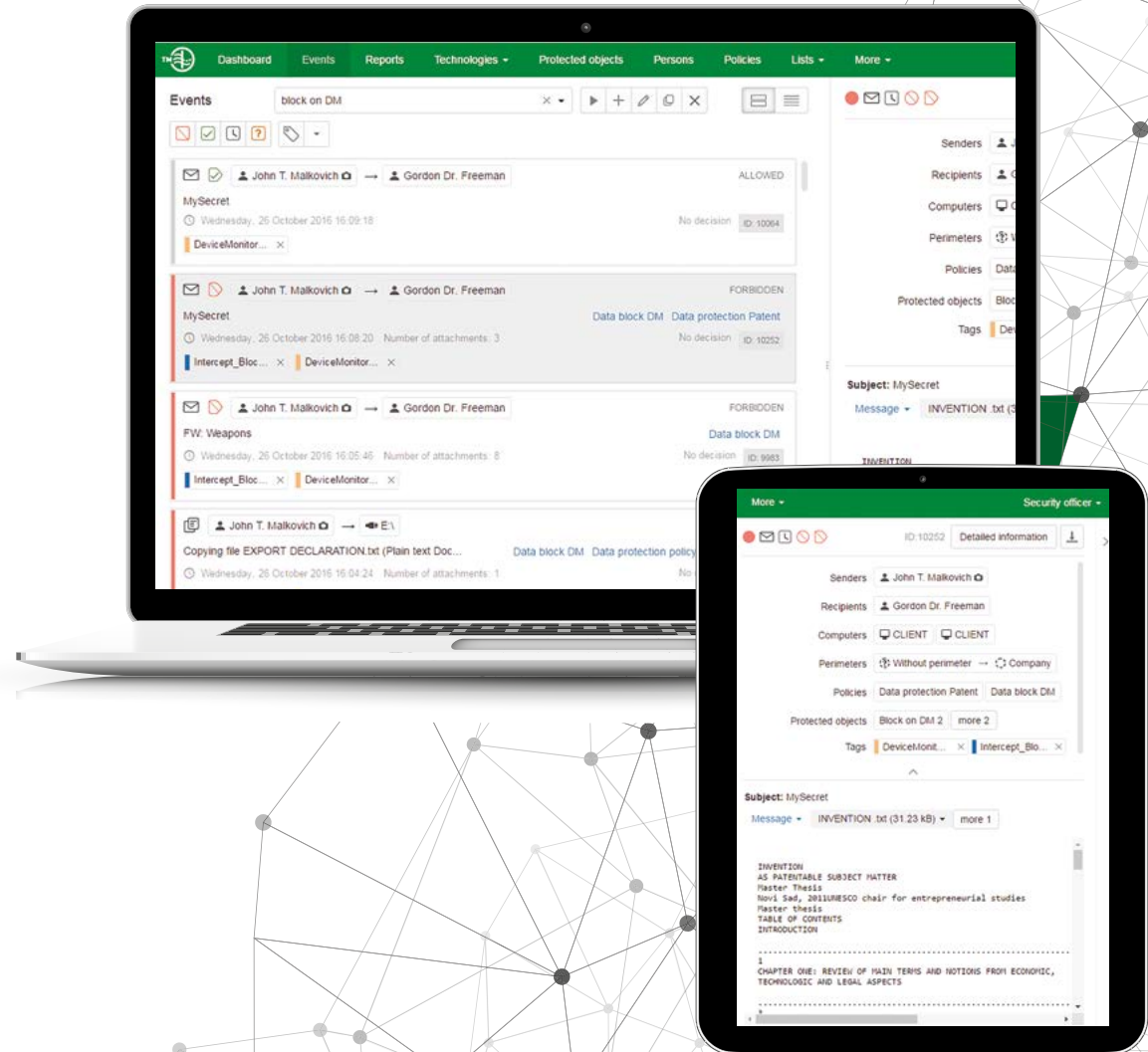


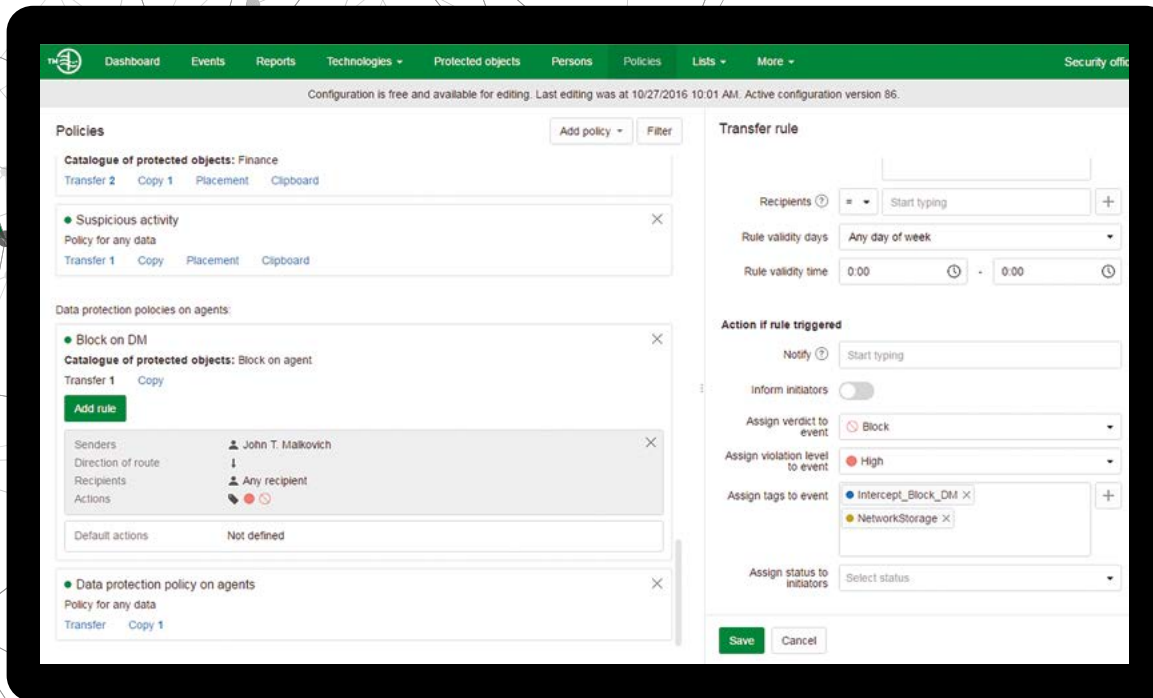
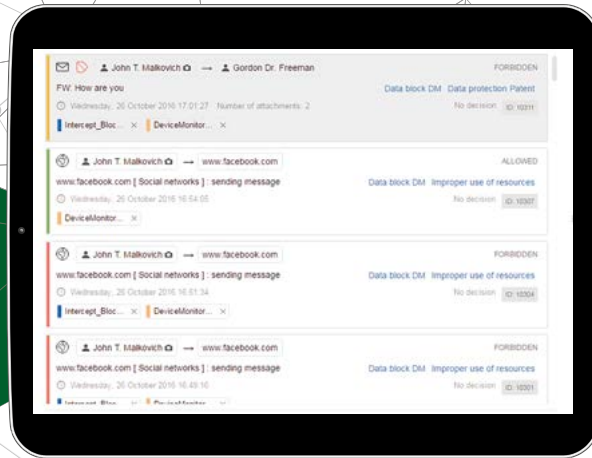
INTERNAL THREATS: FROM NOTIFICATION TO PREVENTION

To effectively address internal threats, it is important to prevent them rather than to deal with consequences.

InfoWatch Traffic Monitor features

InfoWatch Traffic Monitor is a DLP system that immediately blocks violators' actions without interrupting company's business processes, thus preventing internal threats at the time of attack. As soon as a security breach policy is triggered, InfoWatch Traffic Monitor blocks the detected transmission of data under protection. In addition, it bans certain staff groups from performing operations in business applications. E.g., a legal department employee can use a CRM system only to browse customers' details to renew their contracts, but is not allowed to print out such details or take screenshots.





InfoWatch Traffic Monitor allows to

- Block confidential data emailing (both corporate and webmail)
- Block data uploads to cloud storages and FTP servers
- Block postings in social media
- Block data copying to USB drives
- Ban the use of screenshots, clipboard and printing in certain applications

Tasks addressed

- Preventing data leaks in real time without interrupting business processes
- Mitigating financial and reputational risks associated with leak prevention and dealing with their consequences


CONTROL OVER CORPORATE MOBILE DEVICES


Introducing mobile devices to a corporate environment dissolves enterprise network perimeter and makes sensitive data control even more challenging.


InfoWatch Device Monitor Mobile features


InfoWatch Traffic Monitor is a modular solution, with one of its modules, InfoWatch Device Monitor Mobile, protecting corporate data on mobile devices.

 Intercepting SMS and emails, including attachments

 IM communications control

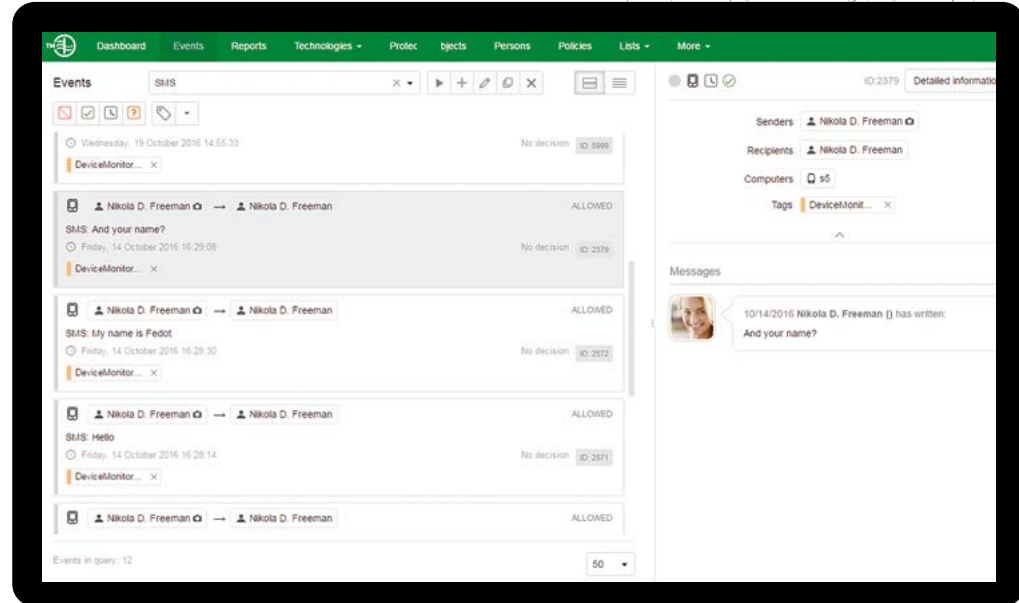
 Intercepting photos taken with a mobile device

 Control over data shared on the web

 Application launch control

Tasks addressed

- Ensuring security even when enterprise network perimeter lacks clarity
- Control over remote and field employees
- Unified security policy management



INFOWATCH TAIGAPHONE

A secure smartphone with trusted Android-based firmware, coming as part of InfoWatch Traffic Monitor and allowing for prevention of corporate data leakage through wireless communication channels.

Mobile workplace

- in-house trusted firmware based on Android
- does not contain backdoors in the software
- does not transfer data to third-party companies

Data transfer control

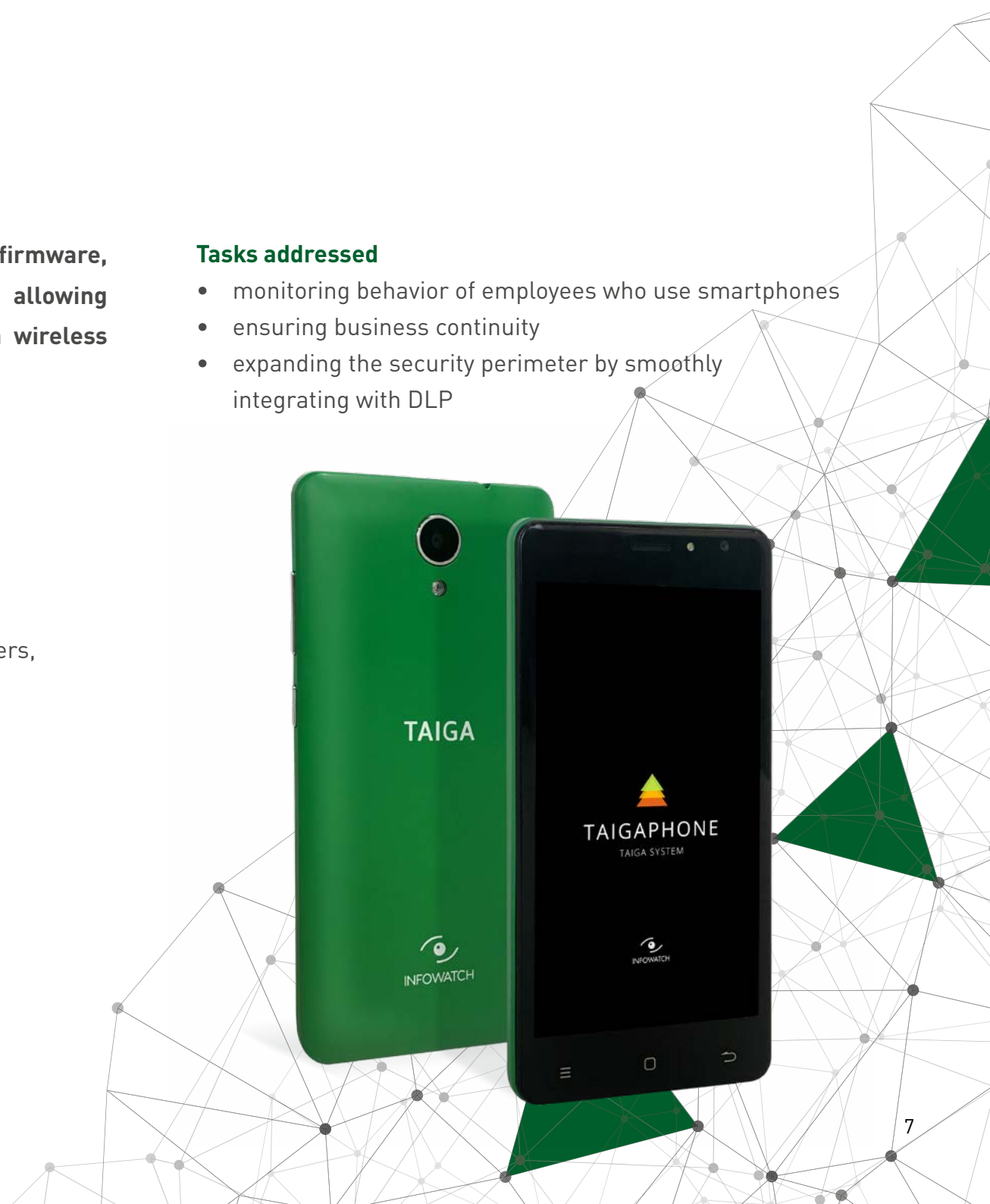
- detection of suspicious conversations in messengers, e-mail apps and SMS
- control of data posted to web resources
- cloud storage monitoring
- capture of camera photos
- capture of media files

Manageability

- centralized application access management via blacklists and whitelists
- control of interface launch: camera, microphone, wireless modules
- LED-light indication for smartphone functions in use (audio recorder activation, Wi-Fi, GSM, etc.)

Tasks addressed

- monitoring behavior of employees who use smartphones
- ensuring business continuity
- expanding the security perimeter by smoothly integrating with DLP



MAP OF INTERNAL COMMUNICATIONS AND EVENTS

Every company faces hundreds of events and incidents daily, which regularly change its information landscape. To keep finger on the pulse, an executive has to see the whole picture of what is going on inside the company. This is what InfoWatch Vision is designed for — visualizing company's information flows and communications.

InfoWatch Vision features

InfoWatch Traffic Monitor is a modular solution. One of its modules, InfoWatch Vision, allows users to see the whole picture of company's information flows, create and keep profiles on employees under suspicion, analyze their social circles, and detect threats in early stages.



Quick and intuitive reports for business unit heads and top managers



Interactive map of employee communications



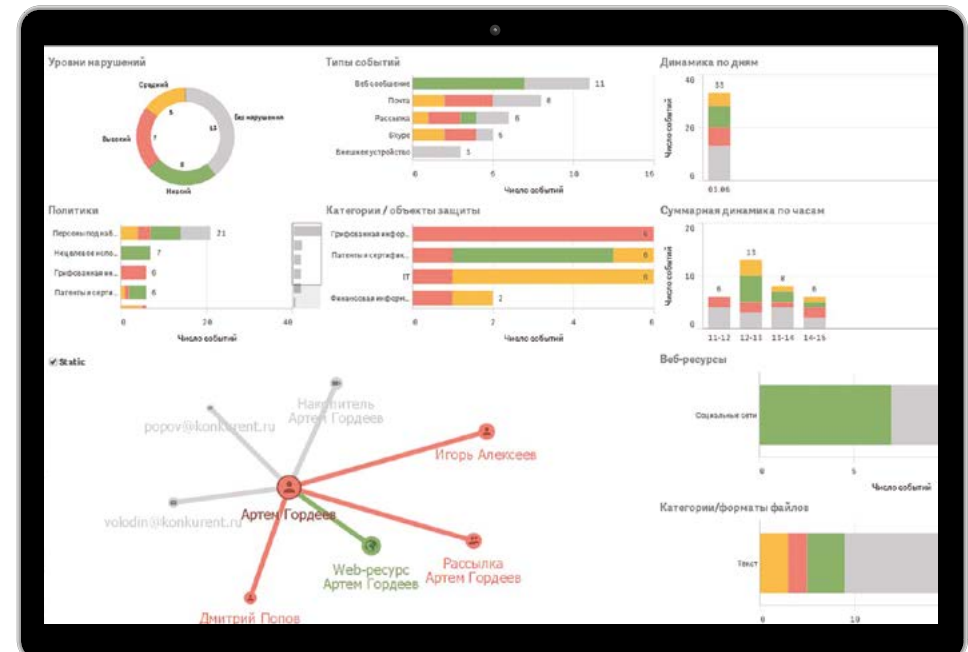
Detailed profile on every employee



Timely identification of risks coming from employees

Tasks addressed

- Targeted control over a group or particular employees under suspicion
- Faster response to incidents and events
- Lower DLP operating costs



PROTECTION OF BUSINESS APPLICATION DATA

Today, companies operate in various working environments, with each business application addressing its own range of tasks and generating large volumes of data. In most cases, data is retrieved from such systems without any control whatsoever, which inevitably leads to the loss of trade secrets and other critical information.

InfoWatch Traffic Monitor features

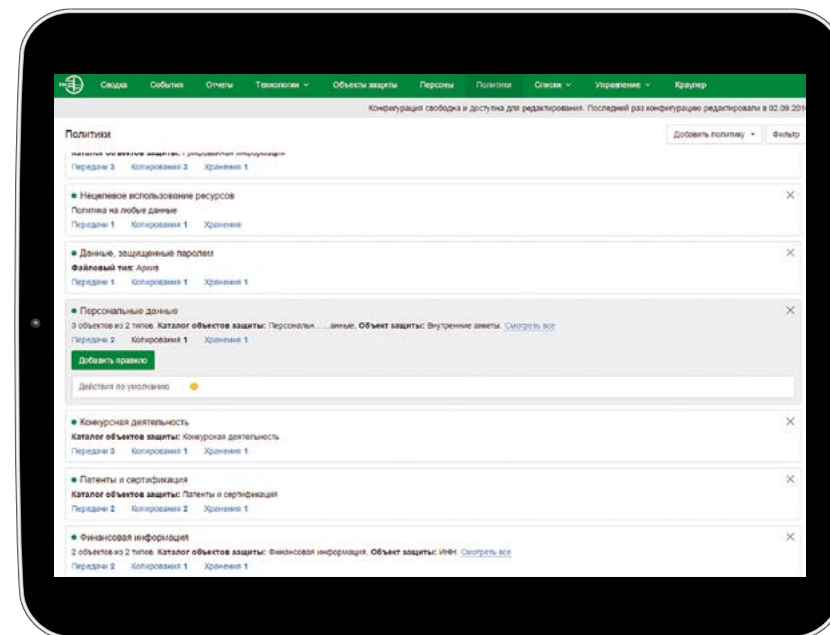
Just like business applications, InfoWatch Traffic Monitor is a full-featured element of a corporate network. It synchronizes with third-party enterprise applications (ERP, CRM), reads their data and runs in-depth analysis using the entire range of analysis technologies and policies. Protection of this data is possible thanks to the InfoWatch Traffic Monitor's open technology ecosystem.

How it works

- upload events from InfoWatch Traffic Monitor to third-party applications
- transfer events from third-party applications to InfoWatch Traffic Monitor
- upload master documents from third-party systems to InfoWatch Traffic Monitor
- intercept HTTP and HTTPS traffic transferred over ICAP

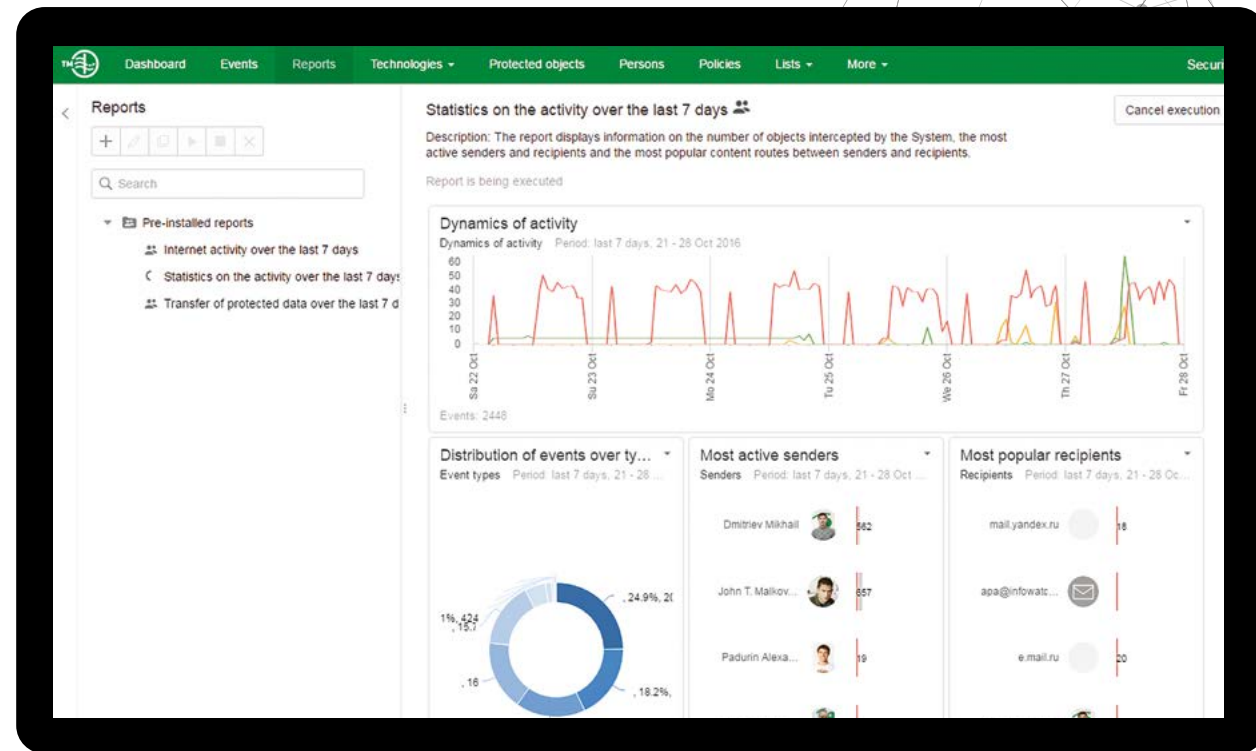
Tasks addressed

- comprehensive approach to combating internal threats, so that no data is ignored by the DLP system
- ease of investigating incidents accumulated in one place and stored in a single archive
- comfort of selecting the business applications to be analyzed by InfoWatch Traffic Monitor and protecting most types of confidential data



BENEFITS

- **Powerful** high-performance solution capable of covering organizations of 300,000+ people
- **Modular structure** allows adding features step by step when needed (add as you grow)
- Out-of-the-box **industry-specific** solutions tailored to meet company's business process specifics, such as content filtering databases for industry sectors like finance, telecom, insurance, government, energy, etc.
- Getting **business units involved** in corporate data security management: HR, legal, marketing, and management can define which employees require closer attention and what information needs extra protection
- Precisely **identifying violators** and bringing them to responsibility using employee profiles and cards, communication graphs



For corporations

Enterprise Edition

- Streamlined for large and geographically distributed companies
- Powerful, high-performance, and fault-tolerant solution
- Perpetual data storage in an archive
- Modular structure with components and scope selected by the customer

For medium businesses

Standard Solution

- For small and medium companies (up to 500 PCs)
- Optimized for the needs of small organizations with minimum setup requirements
- Time-limited data storage in an archive
- Out-of-the-box solution ready for deployment implementation
- Modular structure with components and scope selected by the customer



Vereyskaya Plaza Business Center
29 building 134 Vereyskaya St. 121357, Moscow

www.infowatch.com

+7 (495) 22-900-22

+7 (499) 37-251-74

iw-global@infowatch.com