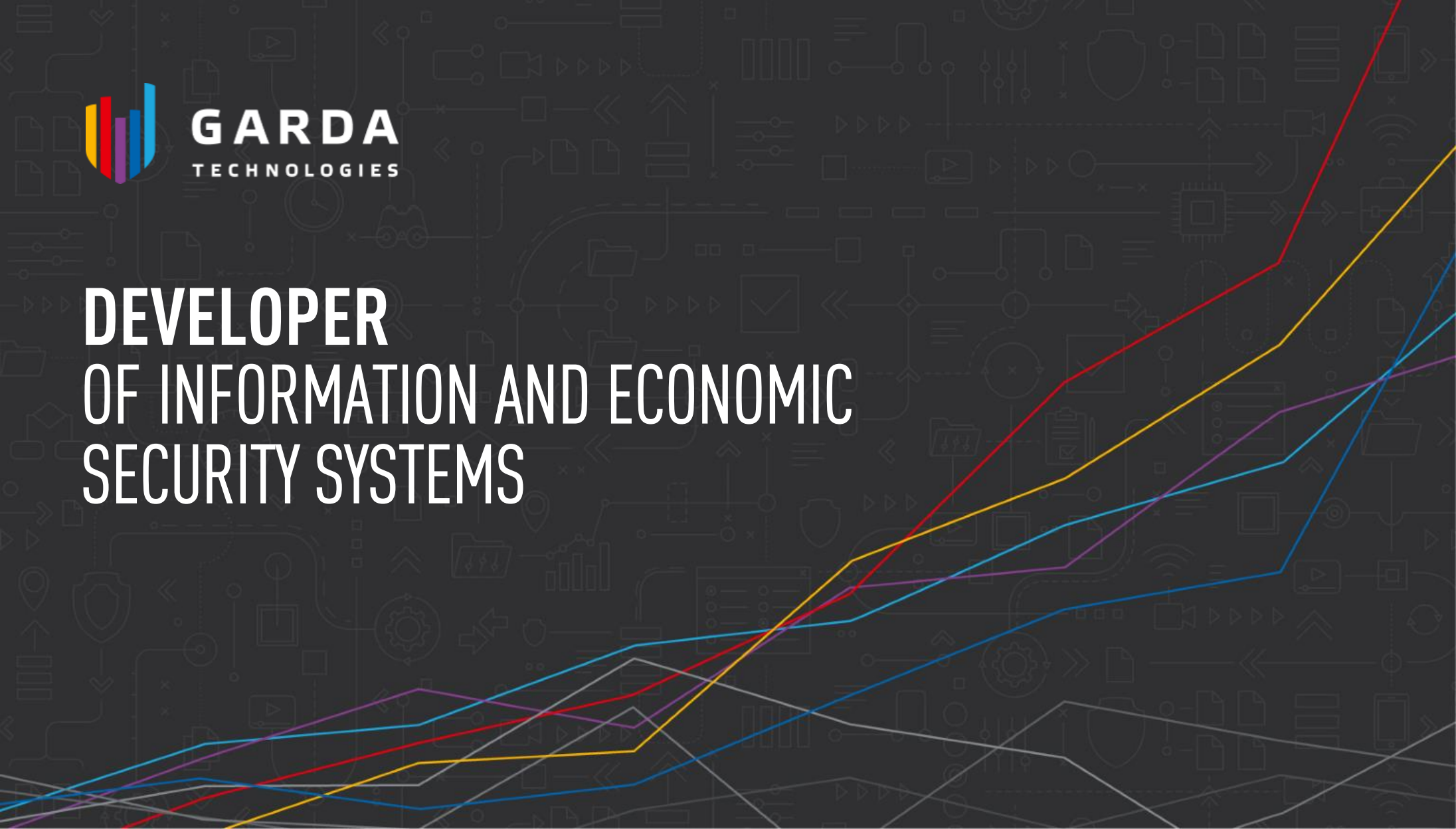

GARDA
TECHNOLOGIES
DEVELOPER
OF INFORMATION AND ECONOMIC
SECURITY SYSTEMS

LET'S GET ACQUAINTED

GARDA TECHNOLOGIES

GARDA TECHNOLOGIES IS A FOREFRONT VENDOR OF INFORMATION SECURITY SOLUTIONS

The company has a long experience in IT industry and focuses on information security.

We've been developing our products since 2005.

Garda solutions are deployed by major financial and industrial companies, telecom providers and governmental institutions.

100 +
deployments

150 +
highly-skilled specialists

12 years
of experience in development of high complexity solutions

5
patented technologies, in-house research centre

PRODUCTS & SOLUTIONS

GARDA TECHNOLOGIES

ANALYTICAL PLATFORM

GARDA ANALYTICS

Development of information and economic security systems.

PROTECTION FROM INTERNAL THREATS

GARDA DB

A system for audit and protection of databases and web applications that prevents possible data leaks and improves reliability of protection.

GARDA MONITOR

A system for network traffic monitoring, detection and investigation of network incidents.

GARDA ENTERPRISE

A system for data loss prevention (DLP) and detection of potential information security threats.

PROTECTION FROM EXTERNAL THREATS

PERIMETER

A group of carrier-grade solutions for prevention, detection and mitigation of DDoS attacks on data networks.

GARDA FILTER

A system for Internet traffic filtering, blocking of access to undesirable domain names, URLs and network addresses.

FRAUD INDEX

A group of solutions for monitoring of transboundary traffic and detection of fraud in the network of a telecom operator.

АНТИБОТНЕТ

Hardware-software complex for analyzing Internet traffic based on botnet signatures.

HOW WE WORK

GARDA TECHNOLOGIES

DEVELOPMENT

Development and implementation for the tasks of the Client

- Prompt development of solutions according to clients' objectives.
- Installation is customized according to network modifications and specific features.
- Selection of the best configuration for the solution.

TESTING

Beta testing.
High speed implementation

- Ample opportunity for beta testing of solutions.
- Minimal delivery time.
- Remote changing of license parameters.

SUPPORT

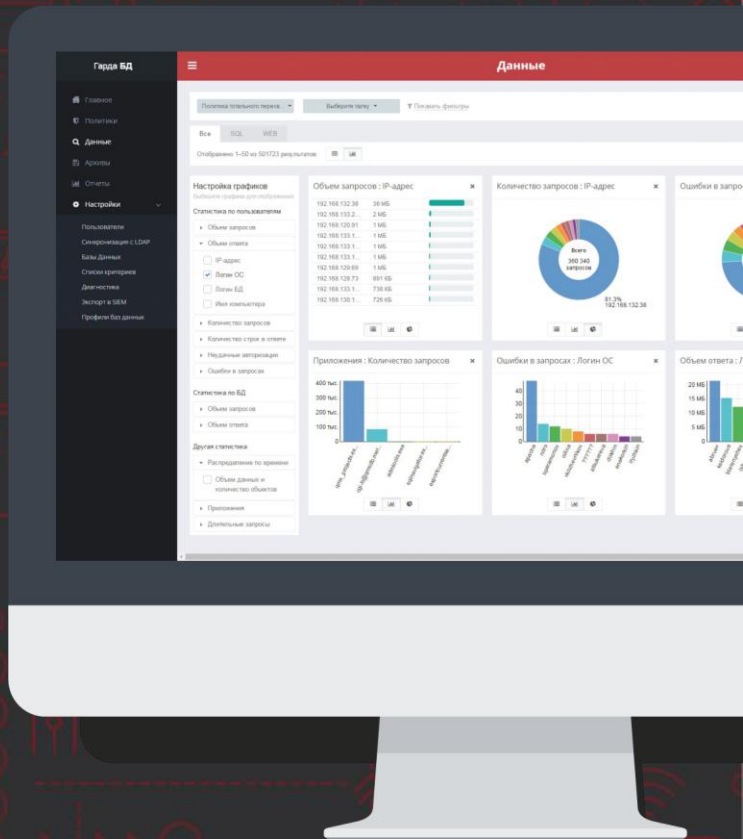
High level customer support

- Unified request processing system in Help desk system.
- 2nd line of technical support – a specialist performs administration tasks.
- 3rd line of technical support – a specialist performs complex settings, makes changes to the operation of IS components if necessary.
- All specialists have degrees in information security.
- High SLA.

GARDA DB

PROTECTION OF DATABASES AND WEB APPLICATIONS

- **Multilevel network traffic analysis**
  detects unknown databases and vulnerabilities in DBMSs.
- **Dynamic profiling based on UEBA** allows to calculate suspicious user actions and to identify anomalies and deviations in their behavior.
- **Intelligent reporting system**
  makes incident investigation simple and quick,
  and the built-in blocking system prevents unauthorized access to data.



DATABASES PROTECTION

GARDA DB

GARDA TECHNOLOGIES

MONITORING AND CONTROLLING OF HETEROGENEOUS DBS FROM A SINGLE CONTROL PANEL

- Supports all popular DBMSs: Oracle, MSSQL, PostgreSQL, as well as WEB applications
- Detects and classifies a database
- Scans a database for vulnerabilities

EVENT ARCHIVE AND INVESTIGATION

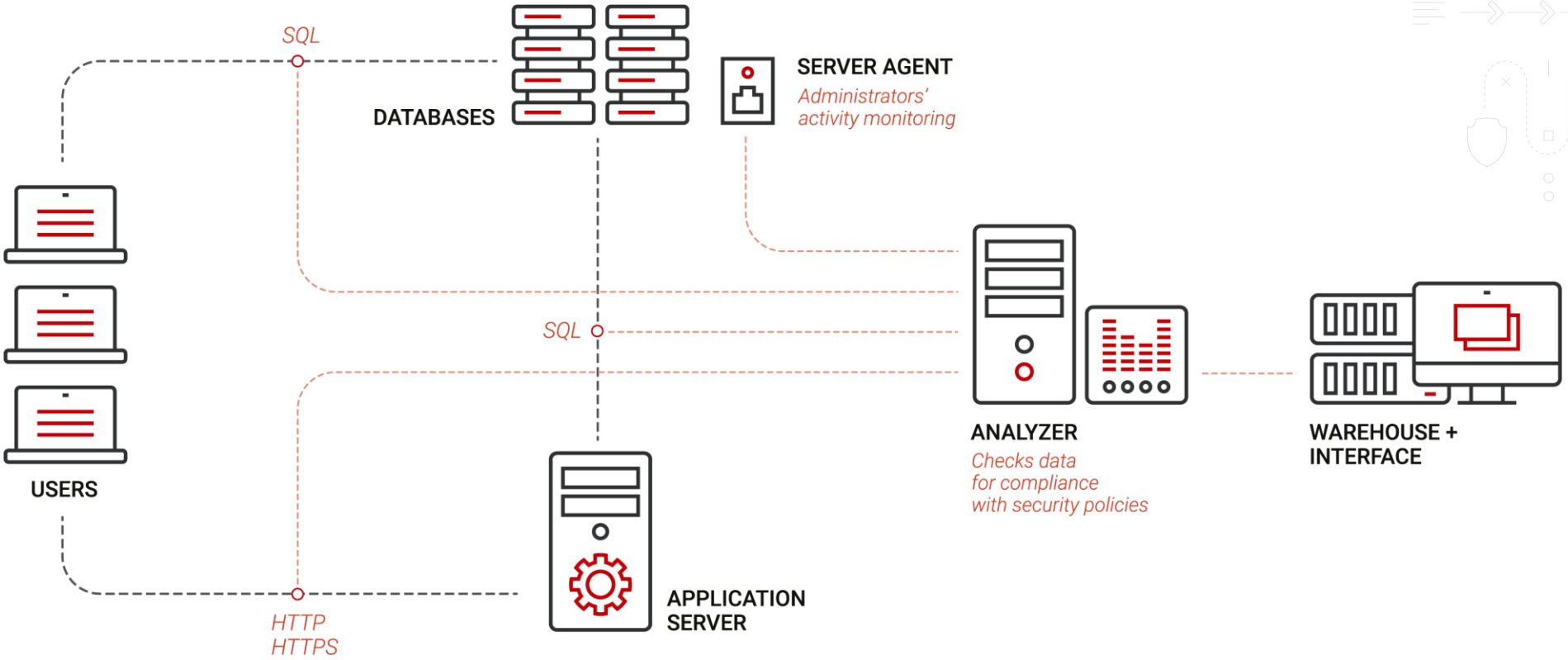
- Total traffic interception for archive and investigations
- Real-time Incident Detection Policies
- Integration with AD, SIEM; email alerts

VULNERABILITIES DETECTION AND ANALYTICS

- UEBA (Behavioral Analytics)
- Building user profiles using machine learning algorithms
- Identification of statistical anomalies and deviations from employees' behavior
- Abnormal activity graphical reports

INTEGRATION INTO A CUSTOMER'S NETWORK

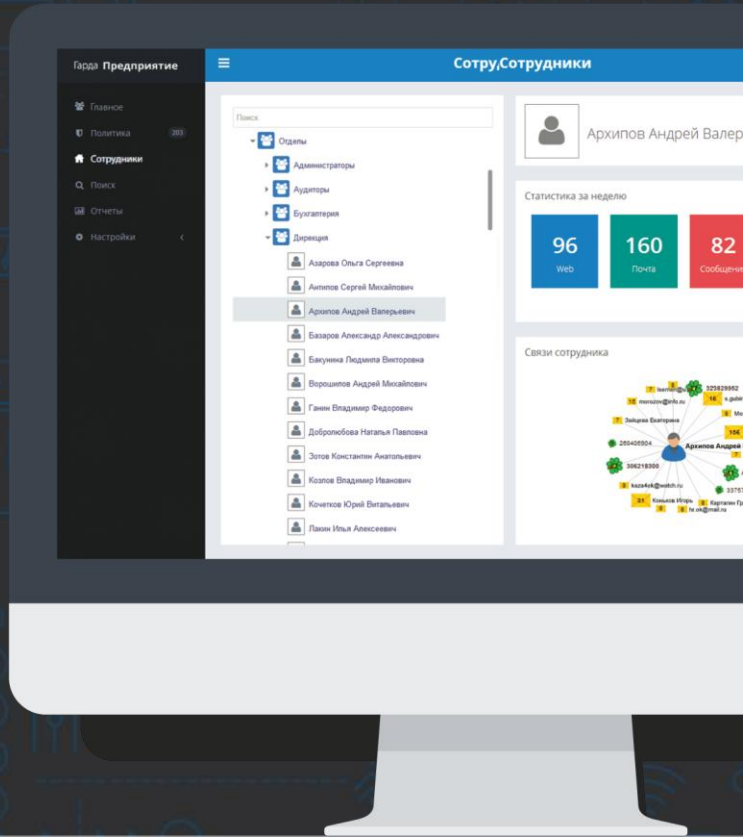
GARDA DB GARDA TECHNOLOGIES



GARDA ENTERPRISE

DATA LOSS PREVENTION SYSTEM

SYSTEM FOR PROTECTION AGAINST INFORMATION LEAKS AND IDENTIFICATION OF POTENTIAL THREATS OF INFORMATION SECURITY



DATA LOSS PREVENTION SYSTEM

GARDA ENTERPRISE

GARDA TECHNOLOGIES

DATA LOSS PREVENTION

- Monitoring of all network communication channels.
- Monitoring of all company's workstations (e.g. Internet searching, key logging, document printing, using of portable data storage devices, VoIP, Skype, Viber, etc).
- Intelligent blocking of incidents.

INTELLIGENT MONITORING AND ARCHIVING OF ALL COMMUNICATIONS

- Instant network communication content viewing for any time period.
- Employees' activities statistics.
- Personal profiles with automatic binding to all accounts.

INFORMATIONAL SUPPORT FOR INTERNAL INVESTIGATIONS

- Automatic reports on security policy violations.
- Data dissemination scheme.
- Employees' contacts.

PROTECTION AT ALL LEVELS

GARDA ENTERPRISE

GARDA TECHNOLOGIES

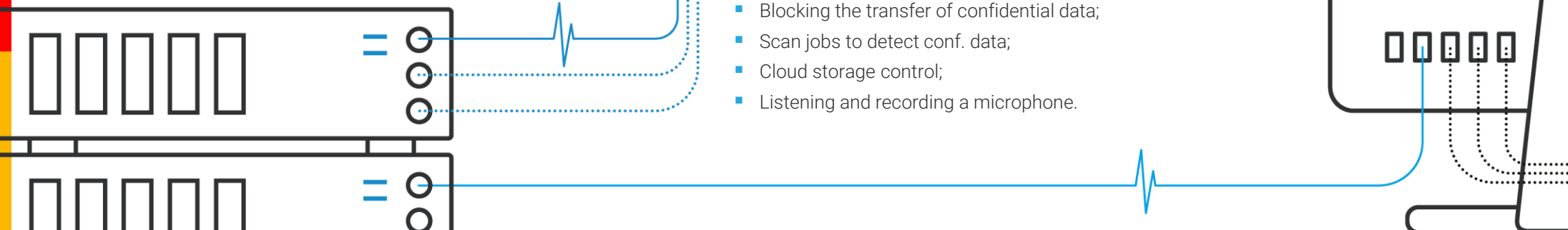
GARDA ENTERPRISE CONTROLS ALL MAIN COMMUNICATION CHANNELS

On the network:

- Email (SMTP, POP3, IMAP, MAPI);
- Visiting sites;
- Uploading data to sites;
- Use of social networks;
- Use of webmail;
- File Transfer (FTP, SMB, Torrent);
- Internet messengers (Lync, QIP, ICQ, Gtalk, MMP, etc.);
- Office VoIP telephony (SIP, SDP, H.323, MGCP, SKINNY, Megaco / H.248).

At work station:

- Shadow copying of data to external devices;
- Print Control (Shadow Copy);
- Desktop screenshots by schedule or condition;
- Viewing the desktop screen in real time;
- Monitoring the use of Skype, Viber, Telegram;
- Keyboard input logging;
- HTTPS control (Social networks, web-mail);
- Application control and activity logging;
- Blocking the use of applications;
- Blocking connected devices (White Lists);
- Blocking the transfer of confidential data;
- Scan jobs to detect conf. data;
- Cloud storage control;
- Listening and recording a microphone.

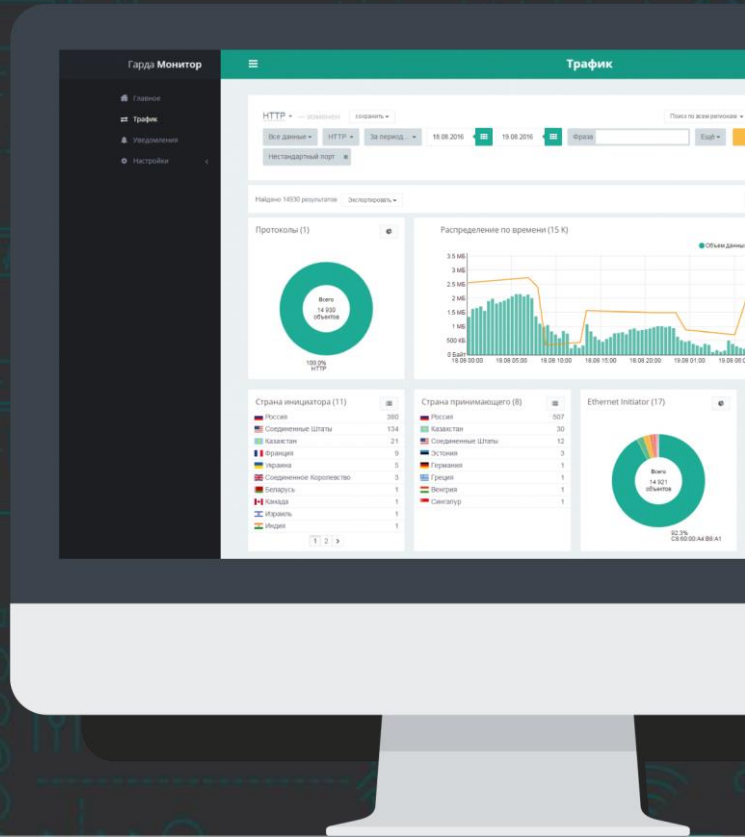


GARDA MONITOR

NETWORK FORENSICS SOLUTION

NETWORK TRAFFIC MONITORING SYSTEM, IDENTIFICATION AND INVESTIGATION OF NETWORK INCIDENTS

Designed to effectively analyze network security events.



NETWORK INCIDENT INVESTIGATION

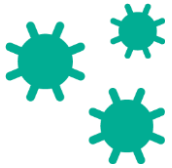
GARDA MONITOR

GARDA TECHNOLOGIES

What happened?

How did it happen?

Who was the initiator?



What poses the threat?

How to avoid it from happening again?

Real-time anomaly detection:

- Spikes or drops in network activity
- Using non-standard ports, protocols, applications

Determining the geographical location of the source and recipient of data

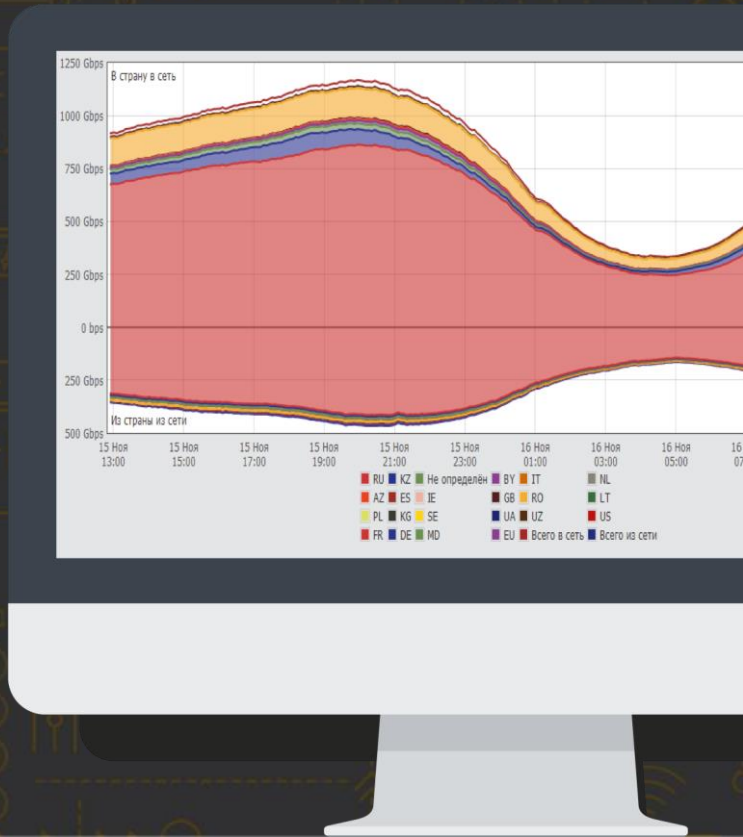
Protocol traffic classification

Record all metadata

PERIMETER

DDOS PROTECTION SYSTEM

- DETECTION AND MITIGATION OF DDOS-ATTACKS
- TRAFFIC MONITORING IN LARGE DISTRIBUTED NETWORKS



DDOS PROTECTION

PERIMETER GARDA TECHNOLOGIES

A CARRIER-CLASS SOLUTION FOR PREVENTION, DETECTION AND MITIGATION OF ALL TYPES OF DDOS-ATTACKS ON ISP NETWORKS AND DATA CENTERS

DETECTION AND MITIGATION OF ATTACKS AND TRAFFIC ANOMALIES

Detects a wide range of network events, identifies and mitigates malicious traffic at high rates.

NETWORK STRUCTURE OPTIMIZATION, PLANNING AND MANAGEMENT

Detailed traffic route information allows the ISP to optimize the internal network structure and interworking with other operators.

RAW TRAFFIC ANALYSIS

The System filters out only the malicious traffic and does not interfere with requests from trustworthy sources.

GARDA FILTER

LOCK PROHIBITED SITES

HARDWARE AND SOFTWARE COMPLEX FOR FILTERING INTERNET TRAFFIC, RESTRICTING ACCESS TO DOMAIN NAMES, URLS AND NETWORK ADDRESSES OF THE INTERNET

The solution is designed in accordance with the Federal Law "On information, information technologies and information protection".

BLOCKING PROHIBITED SITES

GARDA FILTER

GARDA TECHNOLOGIES

Ability to block forbidden pages by URL to prevent the blocking of trusted resources over a common IP

Zero impact on normal user traffic. Only IP requests from the Black List pass through the complex

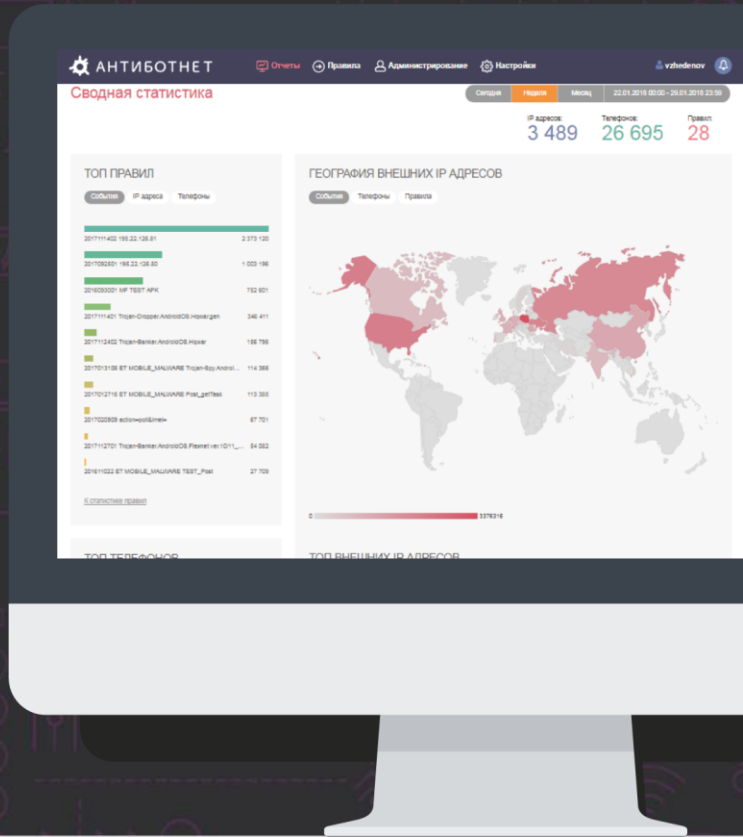
Automate locking and unlocking of prohibited resources

Lock and unlock instantly

ANTI
BOTNET

DETECTION OF INFECTED PHONES

SOLUTION FOR DETECTION OF MALICIOUS ACTIVITY IN THE NETWORK OF A COMMUNICATION OPERATOR AND PARTICIPANTS OF BOT NETWORKS WHICH ACTIONS ARE DIRECTED AGAINST THE OPERATOR'S SUBSCRIBERS



IDENTIFICATION OF INFECTED PHONES

ANTI BOTNET

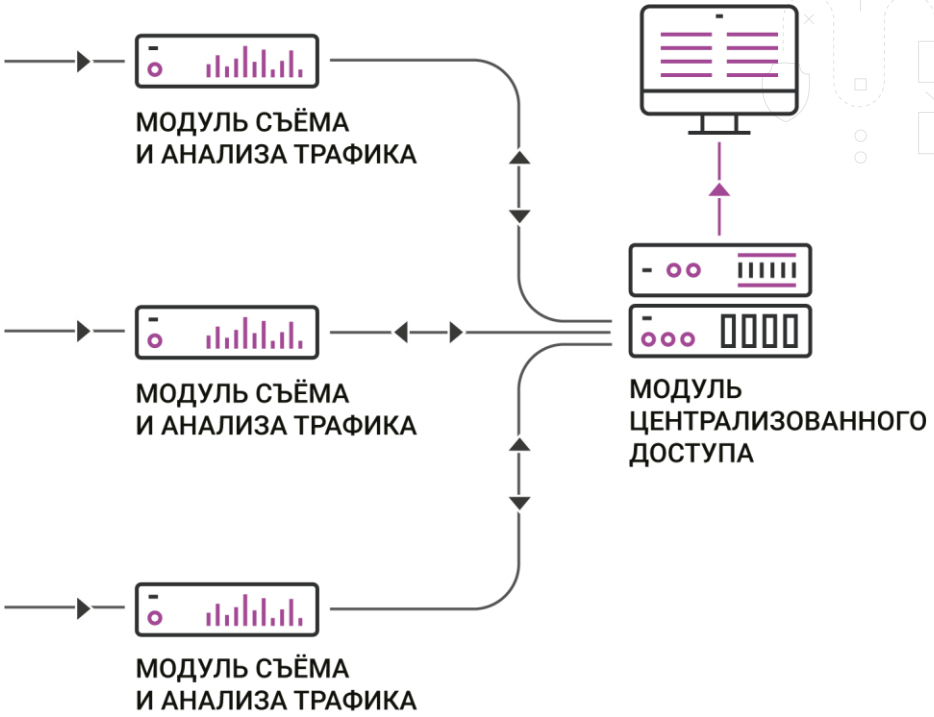
GARDA TECHNOLOGIES

Monitoring of malicious activity of botnets in the network of a telecom operator:

- Facts of malicious activity;
- Infected phones;
- Command centers botnets.

Recording fragments of malicious traffic for subsequent analysis.

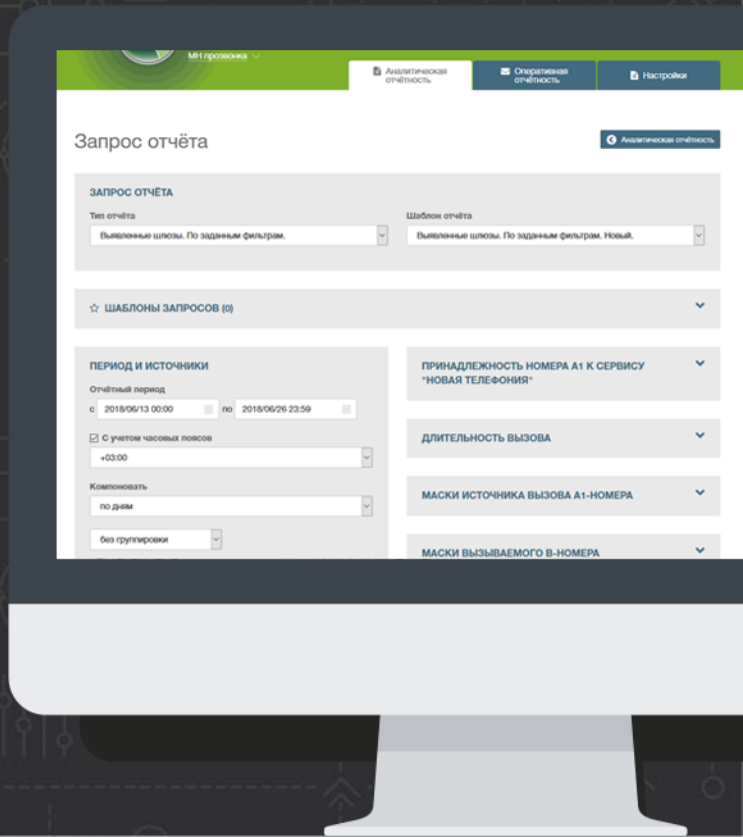
The operator can block access to malicious resources to protect subscribers.



FRAUD INDEX

ANTI-FRAUD AND REVENUE ASSURANCE

A SOLUTION FOR THE DEVELOPMENT OF CARRIER-GRADE AND NATIONAL SYSTEMS TO COMBAT FRAUD IN TELECOMMUNICATION NETWORKS



ANTI-FRAUD & REVENUE ASSURANCE

FRAUD INDEX

GARDA TECHNOLOGIES

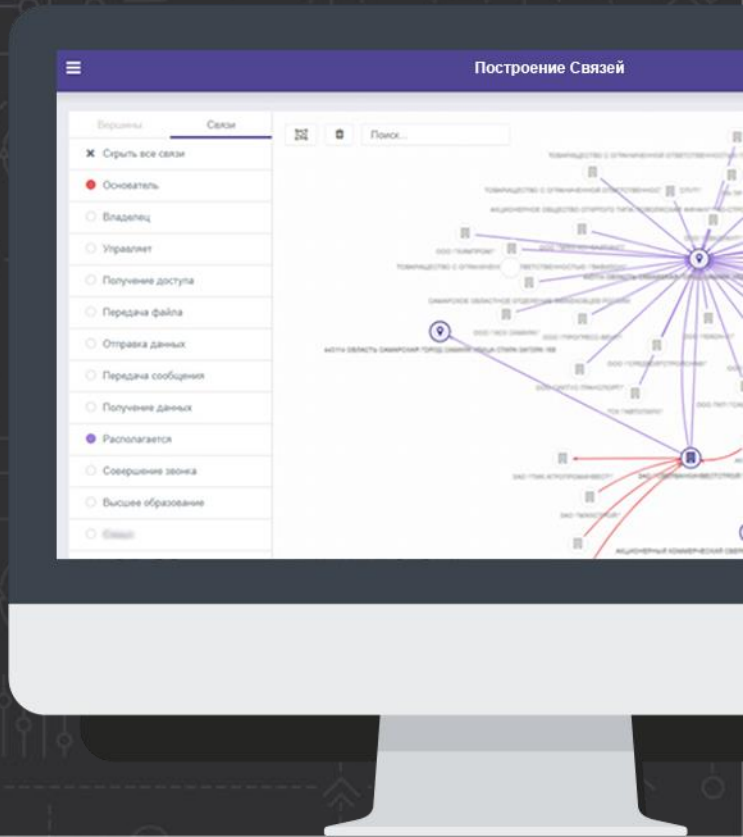
- Monitoring of illegal termination of international voice traffic on the network of a telecom operator
- Monitoring of traffic according to priorities in long-distance and international directions
- Monitoring of illegal pass and sending SMS traffic
- Monitoring of company revenue loss and data integrity in operator's information systems
- Traffic filtering

GARDA ANALYTICS

ГАРДА ТЕХНОЛОГИИ

INFORMATION SECURITY PLATFORM

DEVELOPMENT OF INFORMATION AND ECONOMIC SECURITY SYSTEMS

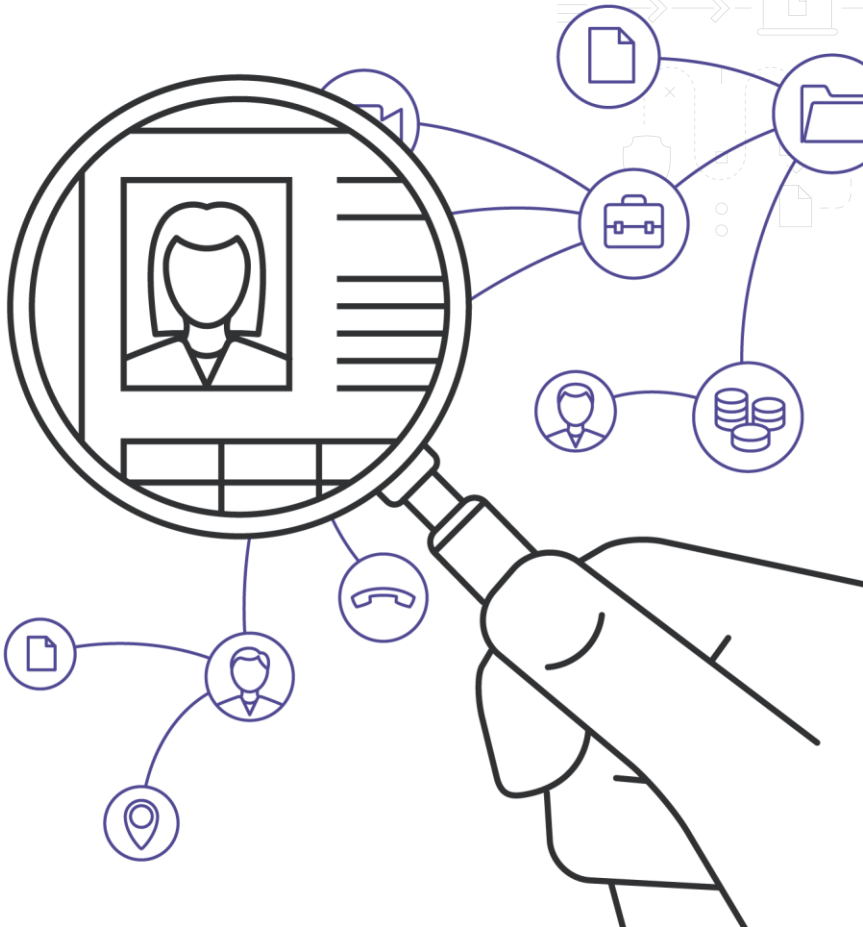


GLOBAL INFORMATION VISIBILITY

GARDA ANALYTICS

GARDA TECHNOLOGIES

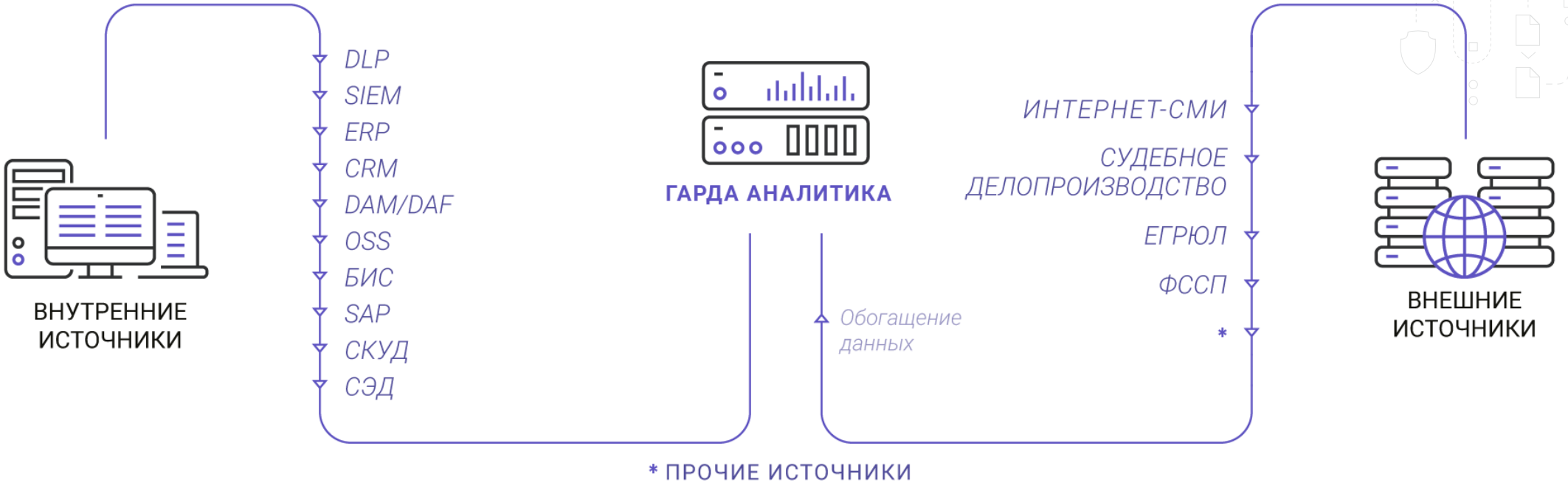
- Monitors risk indicators and security threats
- Warns of the risk of incidents
- Allows you to create incident libraries and replenish them with new risk factors
- Enriches data with information received from external and internal sources
- Provides incident investigation tools
- Analyzes data, fills it with semantic information
- Identifies deviations in the organization business processes
- Keeps all the facts of the organization communications



DATA SOURCES

GARDA ANALYTICS

GARDA TECHNOLOGIES



EXAMPLES OF USING THE PLATFORM

THIS SOLUTION MONITORS AND IDENTIFIES DEVIATIONS IN BUSINESS PROCESSES ACROSS THE ENTERPRISE

EXAMPLES

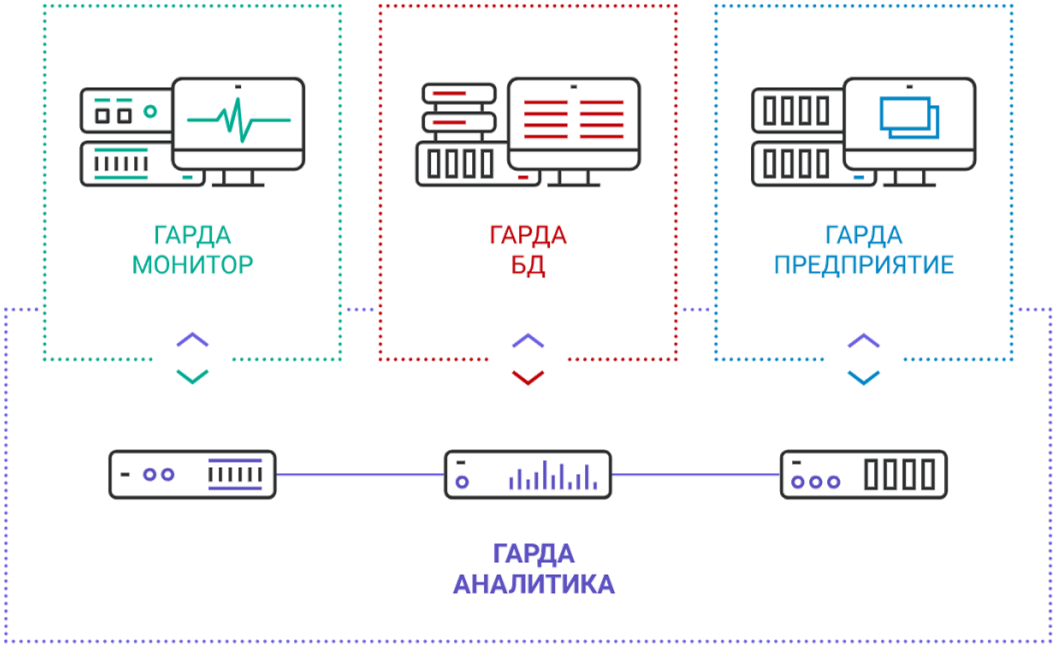
OF TASKS

- Operational assessment of a client, employee, counterparty. Creation of an information base\dossier
- Transactional and telecommunication fraud
- Financial analysis
- Procurement Control
- Production and marketing fraud
- Integrity control and protection of critical data in information systems
- Building device and user profiles Identification of anomalies
- Detection of attacks, infections and shadow information technologies in the network
- Control actions of privileged users in information systems

ECOSYSTEM

- Allows you to quickly create a comprehensive complex to protect the organization from threats to information and economic security
- Minimizes the cost of implementing security systems

ALL SOLUTIONS OF GARDA TECHNOLOGIES ARE COMPATIBLE WITH EACH OTHER AND CAN WORK AS DATA SOURCES FOR «GARDA ANALYTICS» INFORMATION SECURITY PLATFORM



IMPLEMENTATION & SERVICE

ГАРДА ТЕХНОЛОГИИ

PRE-DESIGN SURVEY

- Analysis of business processes and security threats
- Determination of data sources

FORMING A LIBRARY OF SECURITY VIOLATIONS SCENARIOS

- Description of Security Scenarios
- Creating a scripting database

IMPLEMENTATION

- Installation
- Data Sources connecting
- Configuring the platform according to the script library

EXPERT ASSISTANCE

- Audit of business processes for new risks
- Incident Database Update
- Exchange "Best Practices"

ГАРДА
ТЕХНОЛОГИИ

THANKS
FOR YOUR
ATTENTION!

Nizhny Novgorod, Gagarin Ave, 50\9
8 (831) 422 12 21

Moscow, Leninsky Sloboda, 26\5
8 (495) 540 88 10

sales@gardatech.ru

/gardatechnologies

/garda_tech