GARDA ANALYTICS

Big data security analysis (BDSA) that automates incident identification and ensures investigation procedures and early detection of security threats.

Capabilities

- Dynamic data enrichment.
- Human/device behavior deviation identification.
- Explicit/latent relationship establishment.
- Combining various data analysis technologies in one tool.

Global Data Visibility

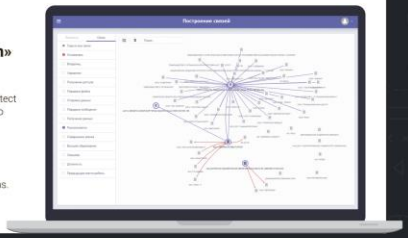
- Monitors risk indicators and security threats.
- Warns on incident risks.
- Allows creating incident libraries and updating them with new risk factors.
- Enriches data with information obtained from external and internal sources.
- Provides tools to investigate incidents.
- Analyzes information, fills data with semantic information.
- Detects workflow deviations.
- Logs communications.

Use Cases

- Operational assessment of customers, employees, counterparties. Database formation.
- Identifying relations between a group of suspects through intermediate nodes in email/messengers/social media/etc.
- Transaction and telecommunication fraud.
- Financial transaction analysis.
- Controlling payments and transfers. Identifying money laundering.
- Procurement control (conflict of interest, relatives, etc.).
- Production and marketing fraud.
- Integrity control and critical data protection in data systems.
- Creating device/user profiles. Identifying anomalies.
- Identifying attacks, infections, and shadow data technologies in the network.
- Controlling privileged users' actions in data systems.

Garda Analytics is a part of «Garda Security Ecosystem»

- Allows prompt creation of a comprehensive system to protect organization against threats to information and economic security.
- Minimizes costs required in implementing security systems.



GARDA TECHNOLOGIES

Garda Technology is a cybersecurity company with experience in developing high-load solutions since 2005. We protect critical systems from cyberattacks and insiders. Our technologies are represented in the major financial companies, industrial and energy corporations, telecom and service providers. All our solutions based on own proprietary technological platform, no third-party licenses required.

Garda Technologies provides integrated implementation and support of data security systems:

- digital assets audit
- vulnerability research
- technical support
- staff training
- post-warranty services

Garda Technologies is part of ICS Holding.

ICS HOLDING

23 COMPANIES
ecosystem of 23 companies providing digital transformation services to enterprises, carriers and national regulators as well as SMEs

$1.5 billion, 700% revenue
growth between 2017 and 2018

1,000 B2B CLIENTS
across over 20 countries worldwide

6,000
highly qualified specialists

CONTACT US TO REQUEST A DEMO OR ORDER A FREE TRIAL

Unit 9, 50 Gagarina Avenue,
Nizhny Novgorod, Russia
8 (831) 220 32 32

antifraud@gardatech.ru
en.gardatech.ru

GARDA TECHNOLOGIES

CYBERSECURITY SYSTEMS

GARDA DB

PCI DSS COMPLIANT

DAM/DBF (Database Activity Monitoring/Database Firewall) Appliance

Database access audit and blocking to ensure DBMS security and independent audit of database and application operations. Continuous database request monitoring. Real-time suspicious operation identification

Capabilities

- Audit of all database operations, including local real-time access.
- Archiving and analyzing database requests.
- Any-period smart data storage.
- User behavior analysis (based on machine learning).
- Automatic active and unknown database identification.
- Data classification by a set of parameters (data location, transfer control, etc.)
- Database vulnerability scanning.
- User right analysis. Access matrix change control.
- Identification of security policy violations (access rights, admin behavior anomalies , breach attempts, etc.).
- Big Data protection.
- Comprehensive graphical reports.
- Blocking undesired user/admin actions.
- Flexible generation of security policies.
- Integration with all popular SIEM systems.

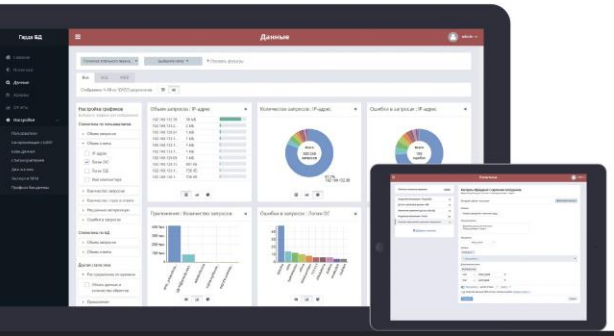
Garda DB protects against intentional or unintentional actions of insiders, hackers, privileged and ordinary users.

Use Cases

- Download and sale of customers' credit card data.
- Fund fraud and thefts.
- Unauthorized access to and sale of private data.
- Manipulations with client bases, KPI cheating by managers.
- Misappropriation and sale of customer bases and other commercial information to competitors.
- Unauthorized deployment of shadow, illegitimate, and uncontrolled copies of critical databases by administrators.
- Others.

Compliance

- PCI DSS
- Basel II
- SOX
- GDPR



GARDA MONITOR

Network traffic analysis (NTA) and Forensics instrument

Ensures transparency of data flows with the help of total control and real-time traffic logging. Identifies anomalies, assists in investigating incidents.

Capabilities

- Flexible filter system. Instant search by criterion (including detection of encrypted traffic).
- Identifying traffic anomalies.
- Determining data source and data recipient locations.
- Storing raw traffic.
- Integration with SIEM systems and data export.
- Full-text search through intercepted data.
- 10 Gb/s traffic analysis.
- 100 Tb+ traffic storage.
- Traffic classification according to 250 protocols (HTTP, POP3, FTP, SSH, etc.)

Network Incident Investigation

- Unlimited volume of traffic registration and any-time prompt access to data.
- Library of preset policies for identifying incidents immediately after implementation.
- Real-time policy customization for immediate traffic control.
- Interactive reports and transparent analytics of incoming and outgoing traffic. Incident statistics.

Traffic Control and Analysis

- Local network IP traffic monitoring and network security incident identification. Analysis of information streams according across relevant protocols.
- Real-time traffic recording for further retrospective event analysis.
- Integrated control center. Aggregated statistics captured from every connection point.
- App-level object reconstruction from traffic.

Garda Monitor ensures complete control of network data flows and allows identifying threats, including cases of breach from an open network into the security perimeter

Use Cases

- Creating user/device behavior profiles. Further identification of anomalies.
- Monitoring network incidents, identifying traces, and collecting evidence during the investigation.
- Tracing network attack sources.
- Identifying malicious software operation and viral activities.
- Identifying resource abuse by employees or unknown third parties (using miner programs, providing access to resources without official registration).

GARDA ENTERPRISE

Ensures data security and confidential data leak protection. Combines classic DLP (Data Loss Prevention) and powerful analytical capabilities.

Major objective: confidential data leak protection caused by intentional or unintentional actions of insiders, hackers, privileged and ordinary users.

Capabilities

- Monitoring network communication channels.
- Automatic incident blocking.
- Centralized management of networks comprising stand-alone DLP systems distributed across company branches.
- Workplace control (Internet, printing, portable media, VoIP telephony, Skype, Viber, etc.)
- Employee schedule control.

Use Cases

- Misappropriation and unauthorized distribution of data.
- Identification of cases of unauthorized forwarding of information related to trade secrets.
- Identification of conspiracies aimed at malicious activities.
- Identification of resource abuse (job hunting, visiting entertainment sites, online games, etc.).
- Identification of the use of inappropriate software (torrent clients, VPN clients, remote access programs, games, etc.).
- Identification of the use of various cloud storage facilities and file sharing services for storing and transmitting operating data.
- Monitoring or blocking the use of portable devices for storing and transferring operation information.
- Revealing facts of contact between employees and competitors (via email, social networks, messengers).

Compliance

- Basel II
- HIPAA
- SOX
- Sec Rule 17a-4