



**GARDA
DB**



GARDA
TECHNOLOGIES

GARDA DB

AUDIT AND PROTECTION OF DATABASES AND WEB APPLICATIONS

A DATABASE ACTIVITY MONITORING (DAM) / DATABASE FIREWALL (DBF) SYSTEM FOR DATABASE ACCESS CONTROL AND AUDIT

Major threats to databases / 3

System overview / 5

- Functionality
- Operating principle
- Integration with the environment

Security policies / 8

- Security policy designer**
- Policy criteria

Database detection and classification / 10

Intelligent monitoring capabilities / 12

- Dynamic profiling
- Active protection. Firewall
- Privileged user monitoring

Technical specifications / 16

About «Garda Technologies» / 19

MAJOR THREATS

**DATABASES KEEP THE MOST SENSITIVE CORPORATE DATA.
ASIDE FROM DATA OWNERS THIS DATA CAN PROVE VALUABLE TO LOTS OF OTHER PEOPLE.**



INSIDERS



Data theft by employees for the purpose of selling to competitors or using it at a new job

HACKERS



The ability to monitor intra-database attacks and back-doors in real time

PRIVILEGED USERS



Privileged activity monitoring

NEGLIGENCE



Unintentional data leaks caused by careless users

REGULATORY COMPLIANCE



PCI DSS



A security standard used by such payment systems as VISA, MasterCard, American Express, JCB and Discover.

The standard describes the procedures, which assure safety of credit card data.

BASEL II



Basel II requires banks to improve their risk measurement and management systems.

The banks are required to manage the location of data, access to sensitive data and tracking usage of data.

GDPR



The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individuals within the European Union.

ISO 27001



ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then.





BUILT-IN AUDITING TOOLS?

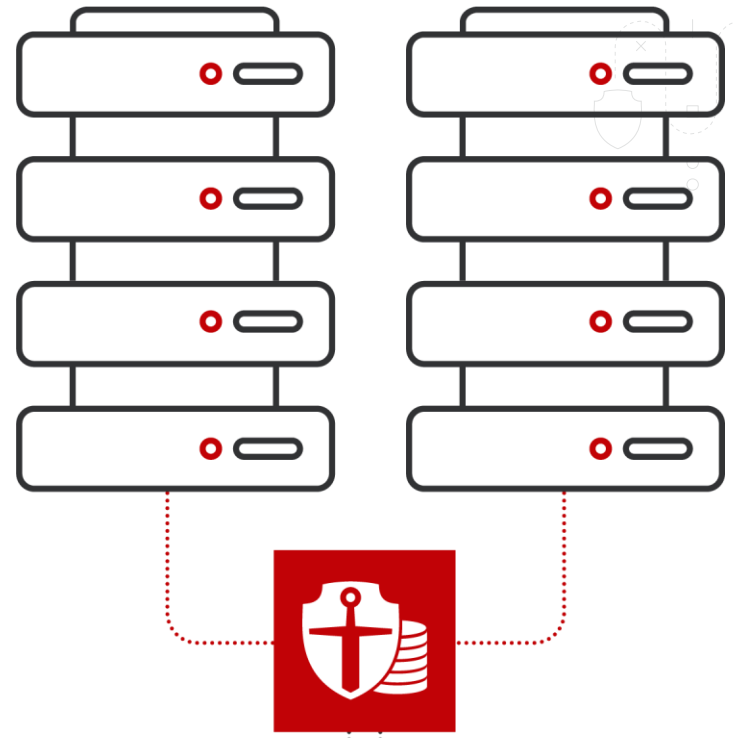
THE USE OF BUILT-IN DB AUDITING TOOLS RESULTS IN ADDITIONAL COSTS BUT DOES NOT PROVIDE THE BEST POSSIBLE LEVEL OF SECURITY

- Requires a special knowledge and constant human monitoring
- 10-40% DBMS performance degradation
- No privileged user monitoring
- No user authentication in a three-tier architecture
- No violation response mechanisms

GARDA DB

A SOLUTION THAT ENSURES DBMS PROTECTION AND INDEPENDENT AUDIT OF DATABASES AND BUSINESS APPLICATION ACTIVITY

-  Protection from leaks of data stored in DBs.
-  Real-time monitoring of DB activity.
-  Monitoring of privileged user activity.
-  Detection and prevention of external attacks.



HOW IT WORKS



1. Traffic analysis

Garda DB analyses network traffic and detects illegitimate user queries and database responses.



2. Long-term storage

Garda DB processes data (e.g., regular expressions matching) and saves all queries and responses for further retrospective analysis.



3. Search for databases

Garda DB automatically searches for new non-monitored DBMSs and classifies them according to the type of data stored in them.



4. Database scanning

Garda DB scans databases and detects vulnerabilities (e.g., non-installed updates, password policy breaches).



5. Analytics/Reports + UBA

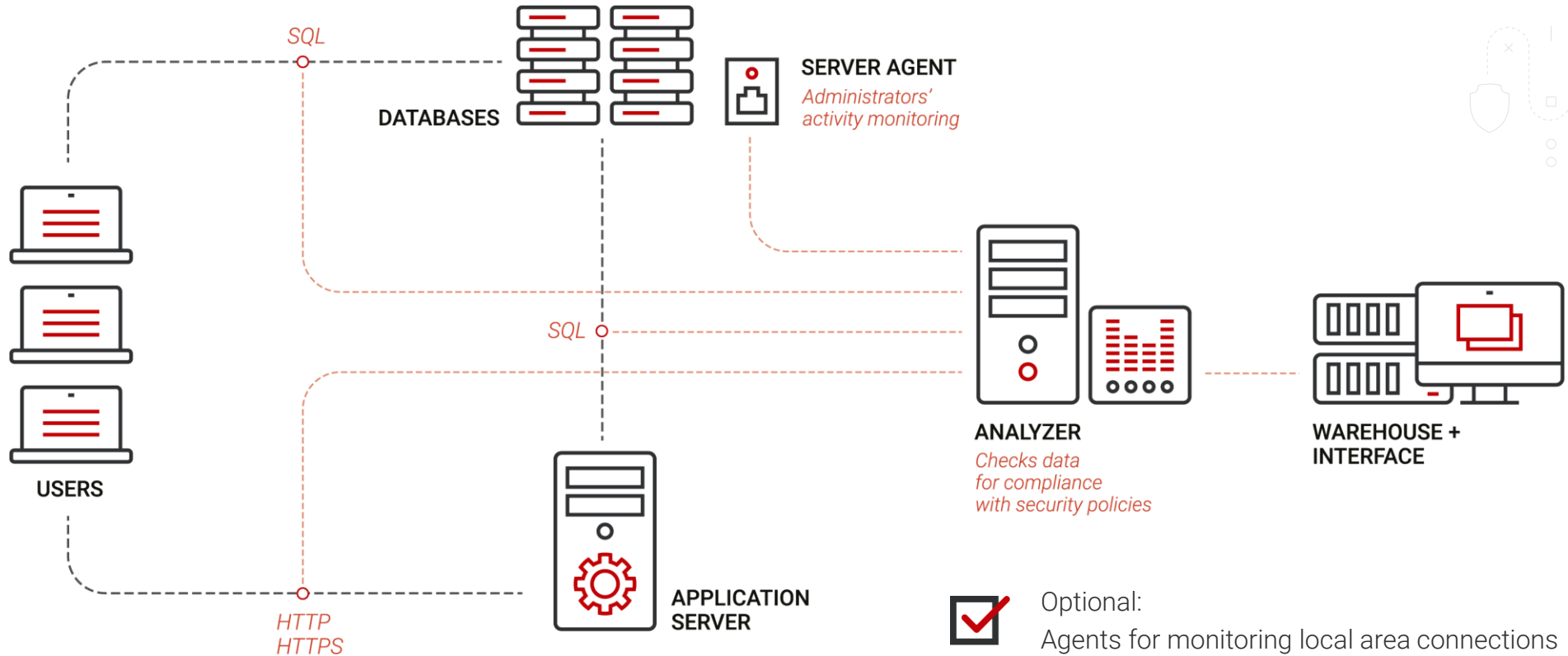
Garda DB detects not only security policy violations but also user behavior deviations.



6. Alerting and reporting

Garda DB provides email alerting, export of data to SIEM and a variety of visual reports on the dashboard.

INTEGRATION INTO A CUSTOMER'S NETWORK

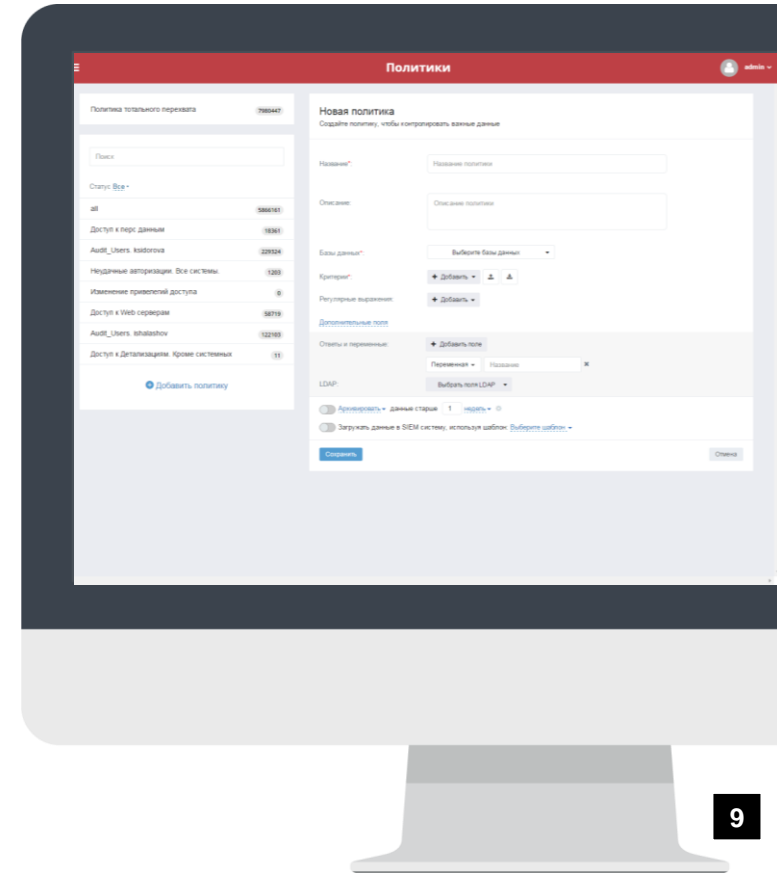


SECURITY POLICIES



SECURITY POLICY DESIGNER SETS THE WAY THE DATA IS HANDLED

- ✓ Wide range of criteria and their combinations
- ✓ Pre-installed regular expressions (personal data, bank cards, etc.)
- ✓ Synchronization with the LDAP server allows adding extra information to captured data
- ✓ Export of processed data to SIEM
- ✓ Backup of captured data by policies



CRITERIA THAT CAN BE MONITORED CONFIGURING SECURITY



- Client's IP address
- DB username
- OS username
- Client's application name
- Authentication output
- Query date/time

- Requested/transmitted table fields, synonyms, views
- Response/query size
- Name of DB object
- Keyword
- Type of SQL command
- Number of rows in response

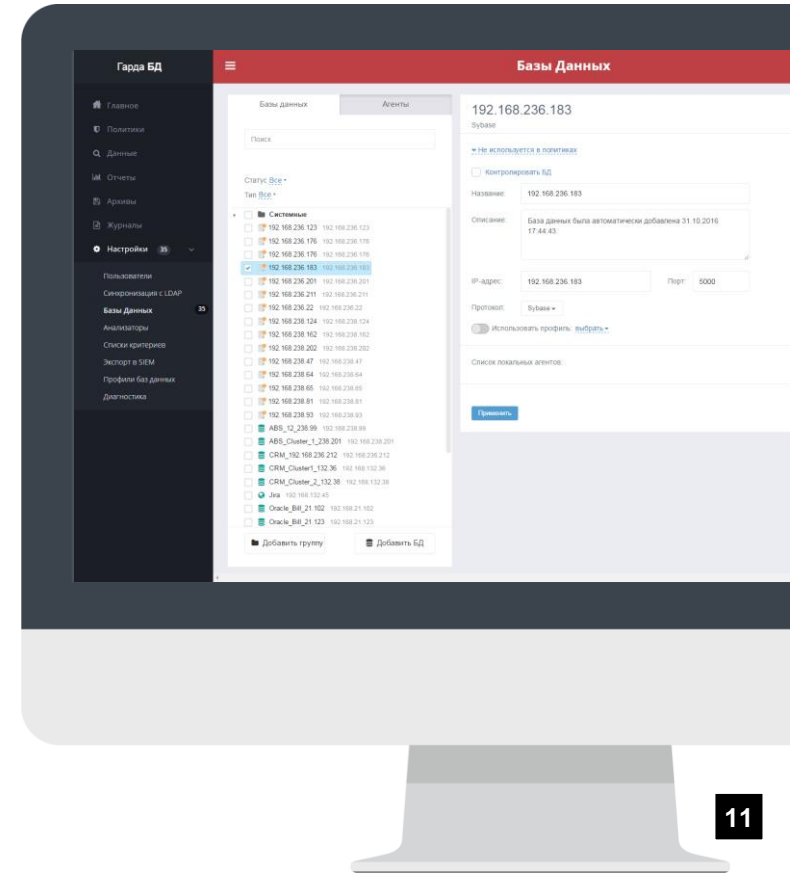
DATABASE DETECTION

THE SYSTEM AUTOMATICALLY SEARCHES YOUR NETWORK FOR NEW NON-MONITORED DATABASES AND CLASSIFIES THEM ACCORDING TO THE TYPE OF DATA STORED IN THEM (E.G., PERSONAL DATA).

According to the data type, Garda DB automatically creates security policies for newly-added databases.

Monitoring can also start automatically.

- Always up-to-date list of company's DBMSs
- Detection of new DBs (creation of new IS/AS)
- Detection of changes in DB IP addresses and ports



DATABASE



GARDA DB SCANS MONITORED DATABASES.

IT GIVES YOU THE ABILITY TO DEAL WITH MORE THAN JUST ACCESS CONTROL ISSUES

CLASSIFICATION



Searching for location of critical information

Creating policies based on scanning results

VULNERABILITIES



Non-installed updates

Checking for optimal DBMS configuration

PASSWORD POLICY



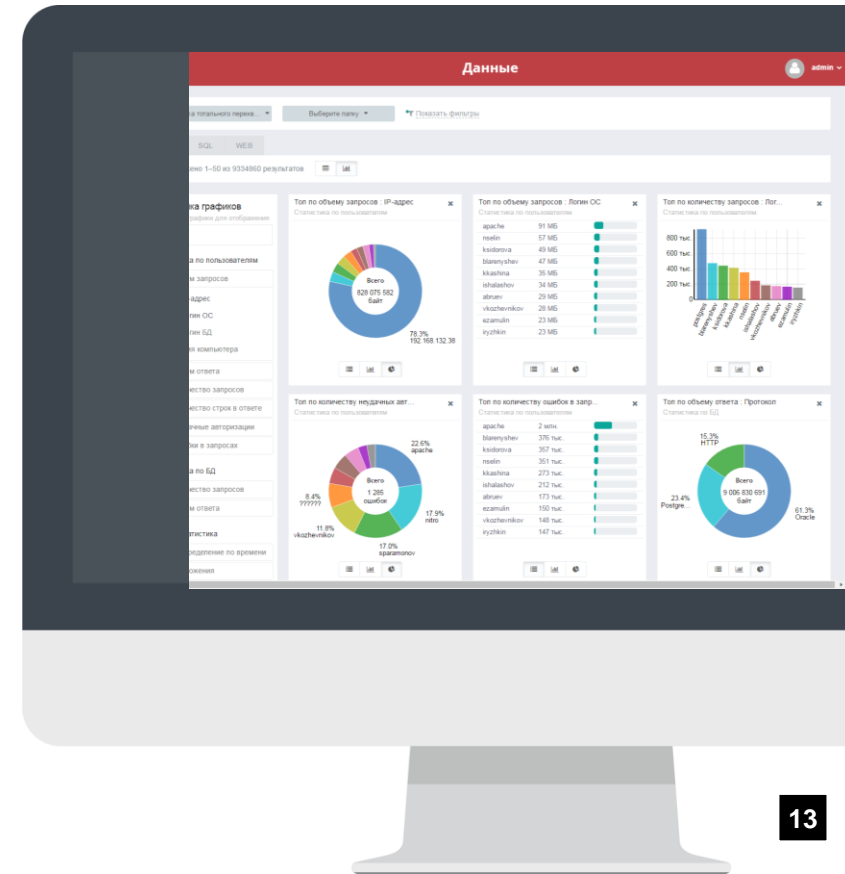
Access control matrix

Policy compliance

MONITORING AND

RICH ANALYTICS TOOLS ALLOW EARLY DETECTION OF DEVIATIONS IN USER DB ACTIVITY (EVEN IF THERE ARE NO VIOLATIONS) AND PROVIDE GRAPHICAL REPRESENTATION OF STATISTICS.

- ✓ Interactive reports
- ✓ Reporting engine can analyze any amount of data for any time period
- ✓ Customizable dashboard
- ✓ User and entity behavior analytics (UBA)
- ✓ Email alerting to violations



DYNAMIC

AUTOMATIC PROFILING IN THE LEARNING MODE

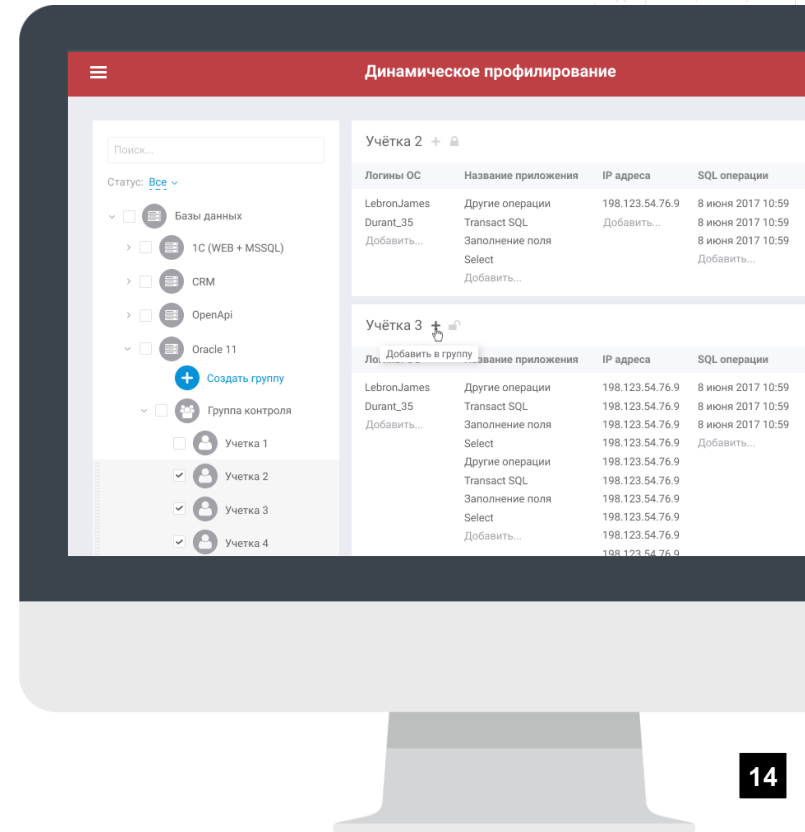


- Learning typical behavior of every user: login names, applications, IP addresses, tables, fields, queries

DETECTION OF DEVIATIONS FROM OPTIMAL PROFILES



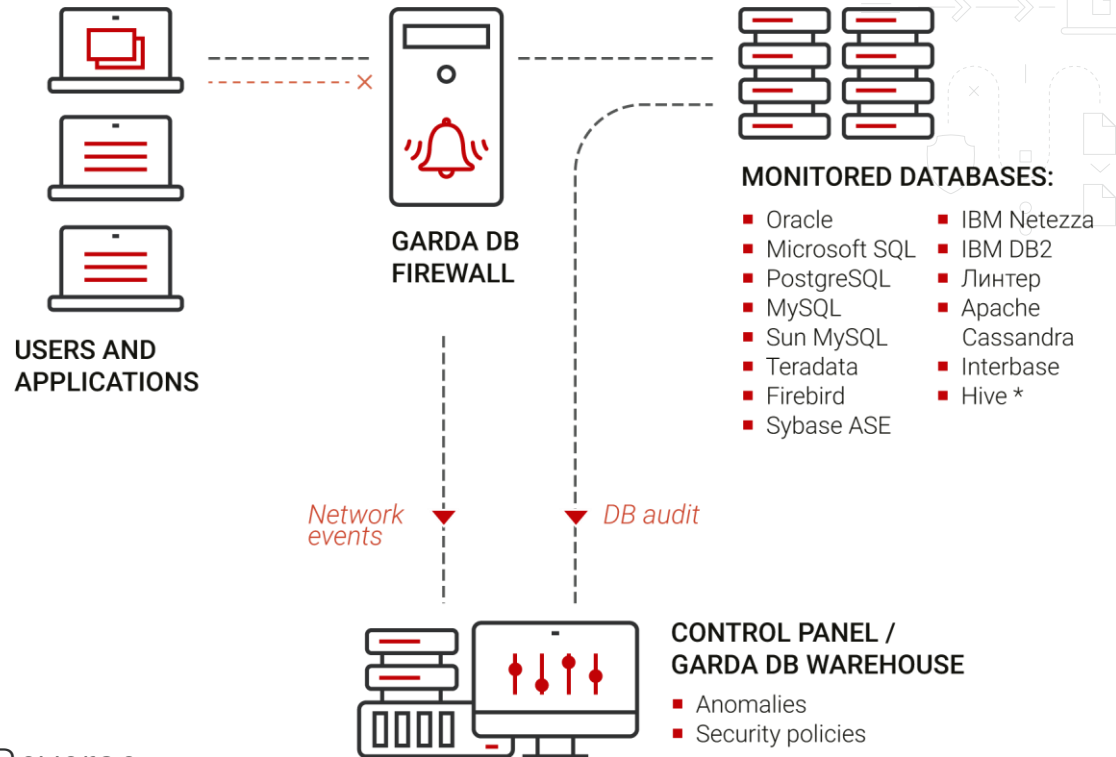
- Suspicious user behavior (Unusual IP addresses, tables, etc.);
- Statistical anomalies
 - Too many queries
 - Too much downloaded information
 - Too many unsuccessful authentications



ACTIVE PROTECTION.

THE SOLUTION BLOCKS UNDESIRABLE USER ACTIVITY THAT VIOLATES SECURITY POLICIES.

INTELLIGENT LEARNING SYSTEM ANALYSES USER ACTIVITY TO PREVENT FALSE POSITIVES.



The blocking is done according to the L3 Reverse Proxy Firewall principle, which results in improved fault tolerance of the system.

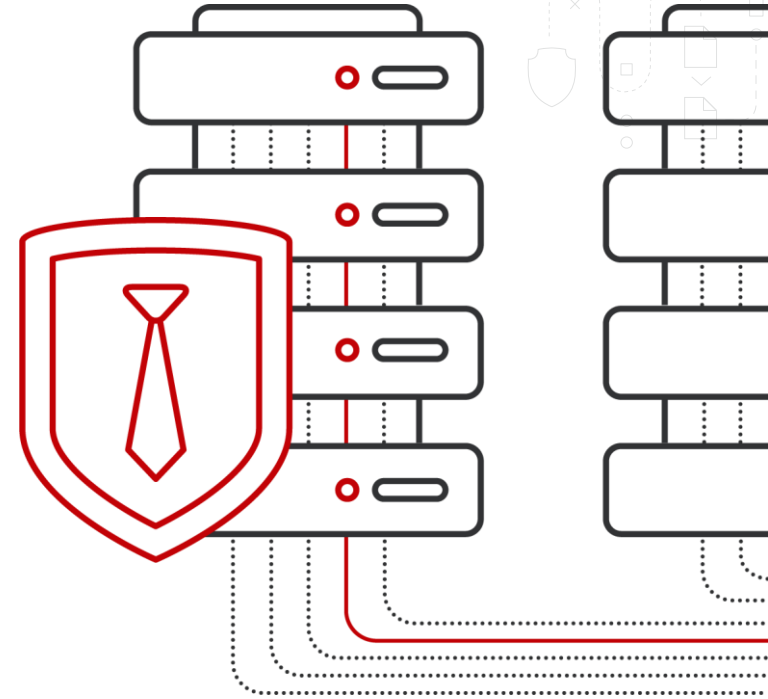
PROTECTION FROM PRIVILEGED USERS



GARDA
DB

GARDA
TECHNOLOGIES

THE SERVER AGENT MODULE MONITORS PRIVILEGED ACTIVITY AND LOGS IT DIRECTLY TO THE DATABASE SERVER.



Innovative technologies of **Garda Technologies** reduced the impact of server agent on the server to increase productivity.

TECHNICAL SPECIFICATIONS

SUPPORTED DBMSs



- Oracle
- Microsoft SQL
- PostgreSQL
- MySQL
- Sun MySQL
- Teradata
- Firebird
- Sybase ASE
- IBM Netezza
- IBM DB2
- Apache Cassandra
- Interbase
- Hive *

*As an access tool to Hadoop

RETROSPECTIVE ANALYSIS



- Total data archiving: all responses, user and application queries. Retrospective analysis for any time period.
- Masking of payment data stored in the warehouse.

USER BEHAVIOR ANALYTICS (UBA)



- Automatic user profiling.
- Deviations and anomalies detection.

WEB APPLICATION MONITORING



- Detailed analysis of HTTP/HTTPS traffic with data extraction from web forms;
- Any web application monitoring:
 - Over the HTTP/HTTPS communication protocols;
 - Over the Kerberos and NTLM authentication protocols;
 - Web form authentication

BIG DATA PROTECTION



DATA MINING

MODERN COMPANIES TEND TO ACCUMULATE MASSIVE AMOUNTS OF DATA FOR MARKETING, SCORING AND OTHER PURPOSES. THAT IS BIG DATA.

NoSQL

BIG DATA IS STORED NOT IN "TRADITIONAL" RELATIONAL TABLES BUT IN SPECIAL HDFS STORAGES. GARDA DB CAN PROTECT THIS DATA.

TEHNOLOGIES

- Apache Hive
- Apache Kafka
- Hadoop
- NoSQL



Monitoring of access to all Big Data systems over Rest API



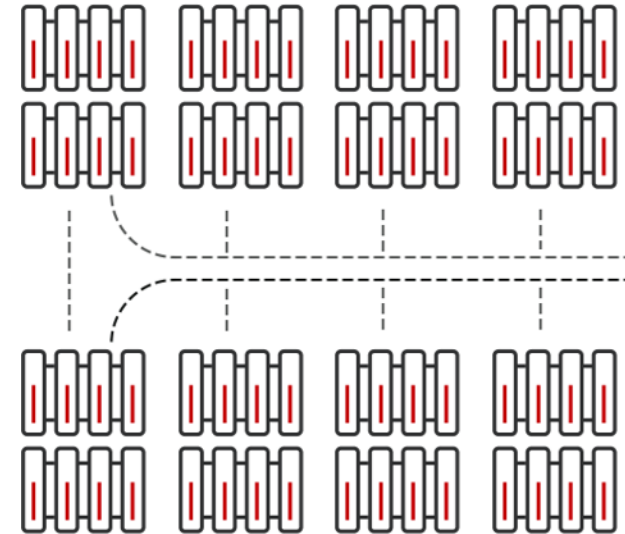
Support Hortonworks Data Platform



Support of HTTP to the data level



Unified approach to relational and NoSQL DBs



A STATE-OF-THE-ART DB SECURITY SOLUTION



MONITORING HETEROGENEOUS DBs FROM A SINGLE CONTROL PANEL

- Creation of geographically-distributed fault-tolerant clusters;
- Automatic detection and classification of DBs in an enterprise network;
- Database performance diagnostics.



INTELLIGENT DATABASE TRAFFIC CONTROL

- Monitoring database queries with synonyms, views and stored procedures;
- DBMS response logging;
- Gathering of encrypted DB traffic statistics.



EXTERNAL ACTIVITY MONITORING

- Detection of SQL injections;
- Monitoring DB queries executed over web applications.



HIGH PERFORMANCE

- 10+ Gb/s traffic analysis rate;
- 40+ TB of data stored;
- Quick full-text search;
- No impact on DBMS performance and business processes.

ABOUT THE COMPANY



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 Technology is a part of ICS Holding

ICS HOLDING



23 companies



\$1.5 billion

700% revenue growth between 2017 and 2018



1.000 B2B clients

across over 20 countries worldwide



6.000

highly qualified specialists



GARDA
TECHNOLOGIES

THANK YOU



**GARDA
DB**



GARDA
TECHNOLOGIES

info@gardatech.ru
+7 (831) 422 12 21
en.gardatech.ru