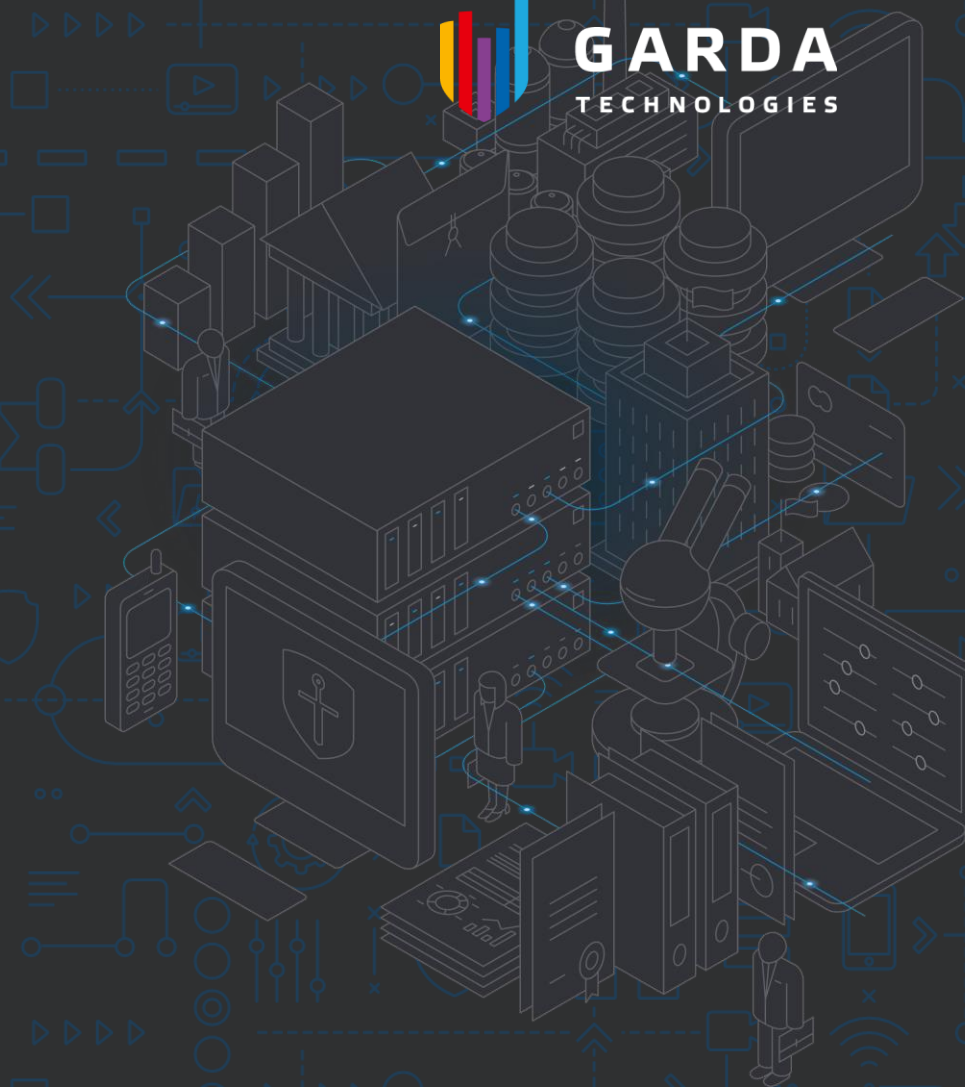




# GARDA ENTERPRISE

SOLUTION FOR DATA STREAM CONTROL & ANALYSIS,  
CONFIDENTIAL DATA PROTECTION AND LEAK PREVENTION



# GARDA ENTERPRISE



**GARDA ENTERPRISE IS A SYSTEM ENSURING DATA SECURITY AND PROTECTING CONFIDENTIAL FROM LEAKS. COMBINES CLASSIC DLP\* INSTRUMENTS AND POWERFUL ANALYTICS.**

\*Data Loss Prevention

## **Garda Enterprise – Fresh DLP Perspective / 3**

### **Features / 4**

#### **Introduction to the System / 5**

- New-Generation DLP System
- General Principles
- System Management

#### **More / 10**

- Implementation Circuit
- Security Policy
- Quick Search
- Search Filters
- Data Warehouse Traffic
- Decoding
- Traffic Transmission Blocking

- Workplace monitoring
- Intercepting and blocking encrypted traffic
- System management

#### **Analytical Capabilities / 21**

- Statistical Reports
- Employee Relations
- Employee Card
- Information Distribution Circuit

#### **Analysis Technologies / 27**

#### **Garda Enterprise Benefits / 28**

#### **Software & Hardware Requirements / 30**

#### **Service / 31**

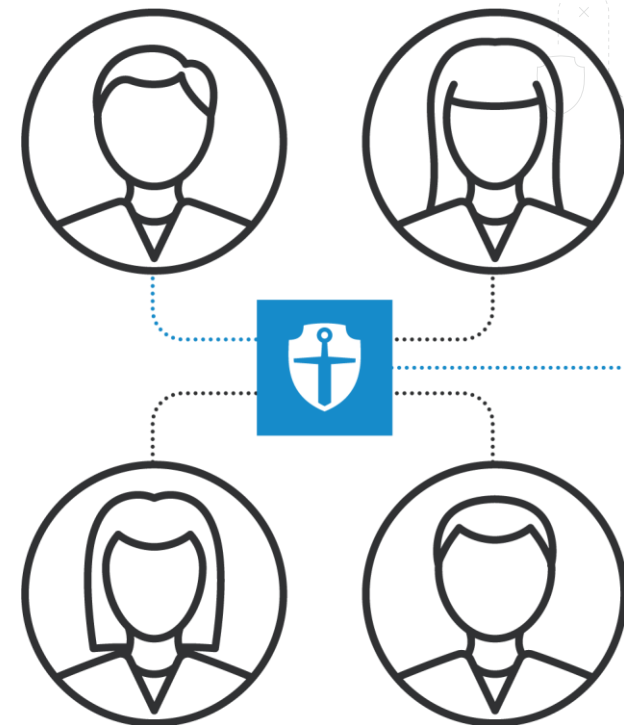
#### **Garda Technologies Profile / 32**

# PURPOSES OF DLP

## MINIMIZE THE DATA LEAK RISK THROUGH MONITORING AND ANALYZING EMPLOYEE COMMUNICATIONS

### GARDA ENTERPRISE BENEFITS:

- Data leak protection
- Identifying intruders and disloyal employees
- Powerful solution for security incident investigation
- Handy management and performance analysis of security policies
- Full staff activity monitoring and analysis
- Workflow archiving



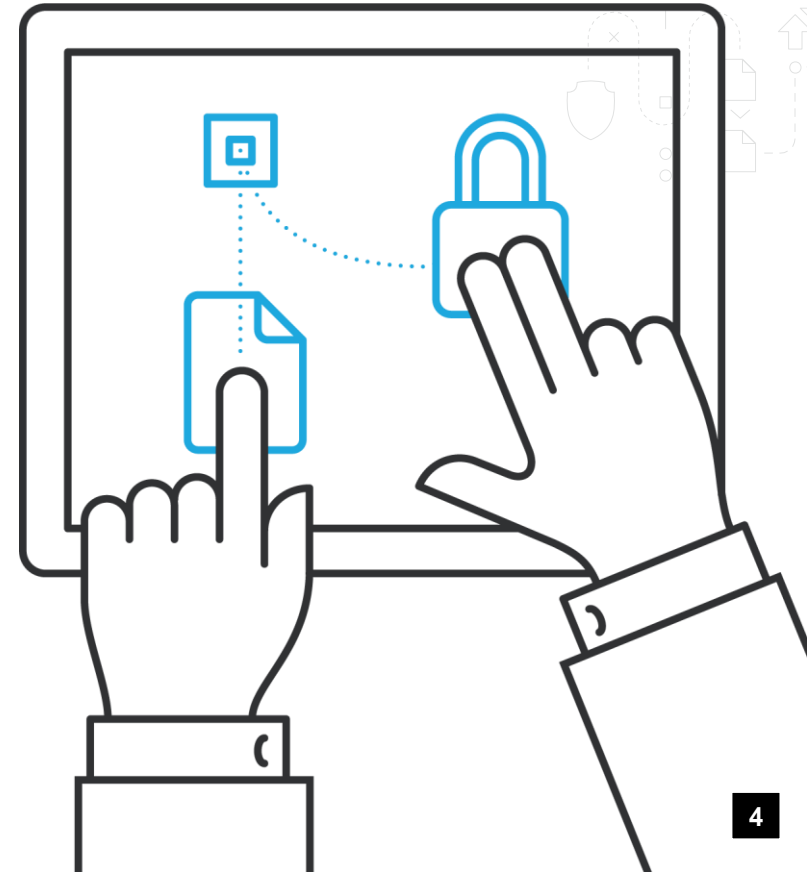
# DLP // MAIN KEY SECURITY INSTRUMENT

**USUALLY, IT TAKES TOO LONG TO CONFIGURE, SUPPORT, AND ANALYZE DLP SYSTEM OPERATION RESULTS.**

**DESIGNED FOR HANDLING DAILY FUNCTIONS OF DATA SECURITY SPECIALISTS, GARDA ENTERPRISE AUTOMATES ROUTINE AND PROVIDES INPUT DATA FOR GARDA ECOSYSTEM**

---

Garda Enterprise identifies violations and threats right after the launch, before finishing the DLP implementation and configuration.



# GARDA ENTERPRISE CAPABILITIES



Multilevel **analytical reports** and **data routes** with fast switching from the general picture to a specific object



Restoring the **full data exchange picture** by any event or document



Storing **all corporate business communications**



Controlling office **VoIP telephony**



Staff **work time analysis**



**Compatibility** with the most common **virtualization environments** (allows for reducing equipment costs and saving system implementation and administration time)



**Controlling** key **communications channel** and data transmission formats (including drawings, torrents, telephony)



**Monitoring network communications.** Managing workplaces from a user-friendly interface.



**Interactive generation** of data security policies ensuring low false triggering



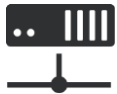
# HOW DLP WORKS

**GARDA ENTERPRISE IS BASED ON THE COMBINATION OF THREE SUBSYSTEMS:**



Interrelated, modules are supplied within an integrated hardware platform.

All software components are Garda Technologies' proprietary solutions that require no further licensing.



## INTERCEPTION & MANAGEMENT

Versatile traffic analyzer that handles network channels and a workplace agent that controls the computer and peripheral devices, allowing various blocking procedures (blocking cloud storages, external devices, processes, etc.)



## STORAGE

Data Warehouse system ensuring optimized storage and quick indexing of all data (messages, files, VoIP calls) circulating within the company.



## ANALYSIS

The system that automatically analyzes data to identify security policy violation incidents and anomalies, and generates reports.



# SECURITY ACROSS NETWORK LEVELS



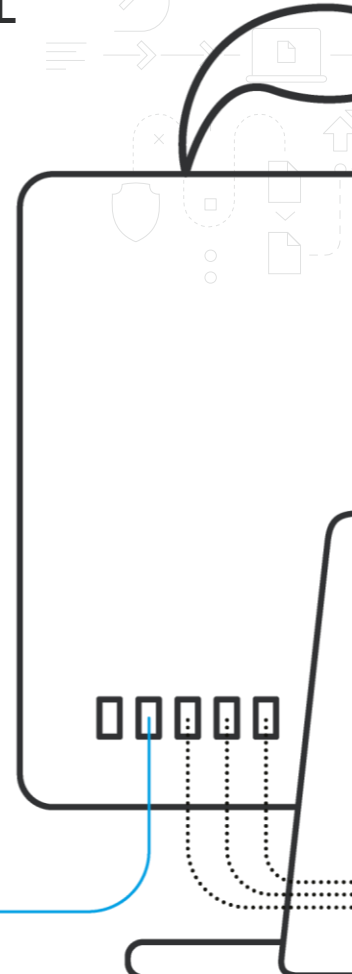
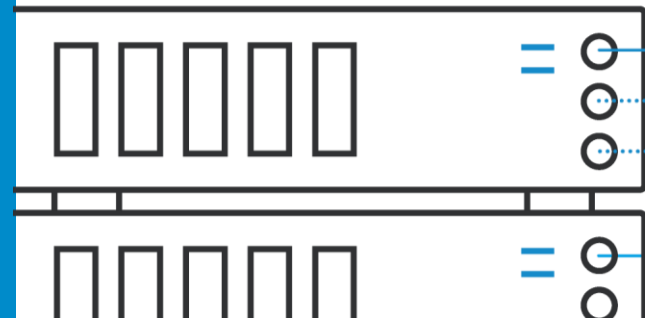
## Workplace:

- Removable media control and blocking
- Printing control (shadow copying)
- Web traffic control (websites, email, social media)
- Messenger control (Skype, Viber, Telegram, Slack, etc.)
- App control and launch blocking
- Cloud storage control
- App usage control
- Confidential document transfer blocking
- Microphone tapping and recording
- Scheduled/triggered screenshots
- Real-time screen monitoring
- Keyboard input interception
- Workplace document search (crawler)

## GARDA ENTERPRISE HELPS CONTROL ALL COMMUNICATIONS CHANNELS

### Corporate network:

- Email (SMTP, POP3, IMAP, MAPI)
- Visiting websites
- Uploading data to websites
- Using social media and email
- File transfer (FTP, SMB, Torrent)
- Internet messengers (Lync, QIP, ICQ, Gtalk, MMP, etc.)
- VoIP telephony (SIP, SDP, H.323, MGCP, SKINNY, Megaco/H.248)
- Integration with the company's Active Directory
- Integration with the proxy server over ICAP
- Intercepting Skype for Business messages
- Corporate email control
- Drawing detection (CAD)
- Detecting sealed documents
- Intercepting VoIP calls
- Identifying passport, credit card, driver's license scans



# USE CASES

- Controlling corporate data streams
- Controlling workplaces
- Data security incident tracking and Prevention
- Early identification and prevention of data leaks

- Inappropriate action blocking
- Staff work time control
- Incident investigation
- Archiving data for further retrospective analysis



---

## COMPLIANCE



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



# SOLUTION STRUCTURE

## GARDA ENTERPRISE

## SOURCES



Corporate Email  
Server

Proxy Server

Active  
Directory

Skype  
for Business  
cepber

SPAN

### WORKPLACE AGENTS

- Windows
- Linux
- MacOS

### DATA PROCESSING & STORAGE SUBSYSTEM

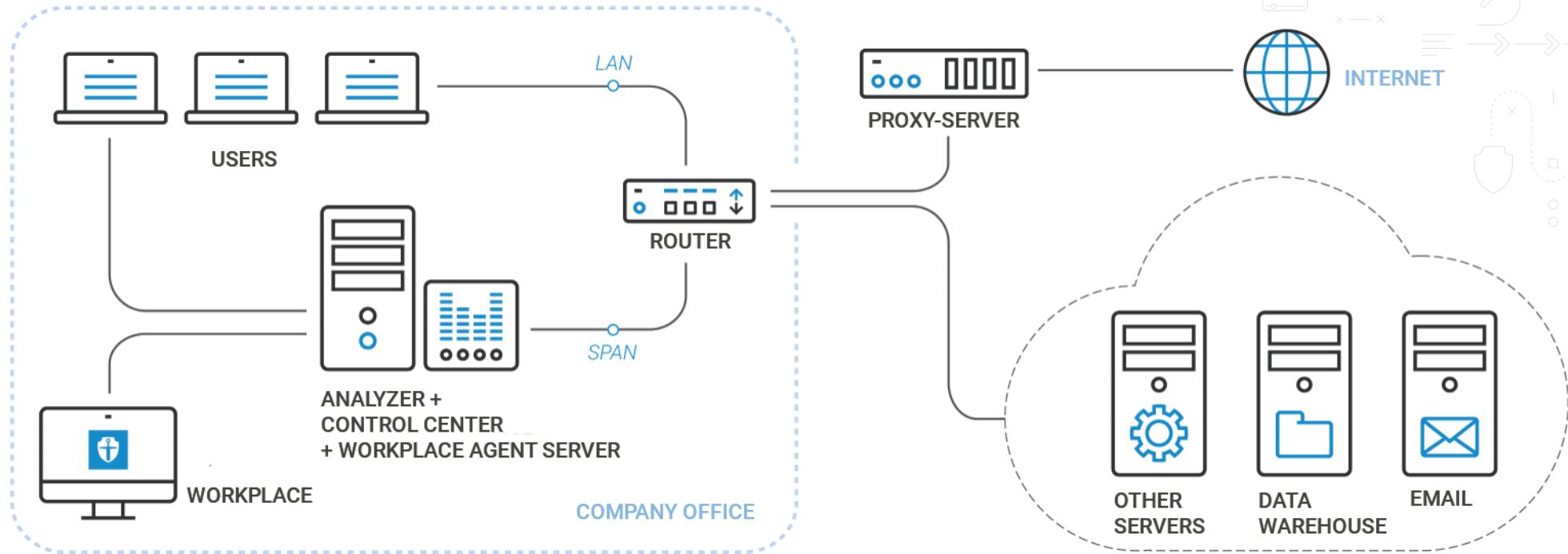
- AGGREGATION
- DECODING
- STORAGE

### MANAGEMENT SUBSYSTEM

- CONFIGURING
- INCIDENT HANDLING



# IMPLEMENTATION CIRCUIT



System functions—including workplace agent management, HTTPS handling, traffic interception and analysis, data storage—are provided on a 1U/2U OR 4U server (depending on the number of workplaces and storage period).

# CAPABILITIES || #1



## Related document search

Searching for text documents based on the preset samples. Immune to changes made to the document and copying of large text fragments to another document.



## Data storage and analysis

Big data storage and handling methods allowing for superior system performance and intermediate criterion-based and full-text search.



## Encrypted traffic control

**Workplace:** DLP agent, unnoticeable, autonomous, and light.

**Network:** encrypted connection proxying module installed in the gap of the controlled data transmission channel.



## Search by criteria

- Searching for information based on signature and other non-text criteria: data type (data exported from databases, file types), data volume, transmission protocol, employee credentials, etc.
- Searching for documents and document fragments in data transferred by employees.
- Identifying structured data in the data stream (ID card numbers, card numbers, emails, etc.)
- Optical character recognition for further analysis



## Geocluster

Centralized management of the network comprising standalone DLP systems distributed across the company branches.



GARDA  
ENTERPRISE

GARDA  
TECHNOLOGIES

# CAPABILITIES || #2



## Workplace peripherals control

USB carriers, black and white device lists, information blocking and shadowing.



## Data transmission blocking

Proprietary file labeling technology allowing for blocking and tracking document transfer.



## Banned resource blocking

Controlling and blocking access to specific resources or resource groups.



## Cloud app control

Monitoring and controlling access to cloud drives and apps



## Crawler

Identifying confidential data at work stations and in network warehouses.



## Workplace app control

Controlling access to categories and individual apps. Analyzing app/category activity.

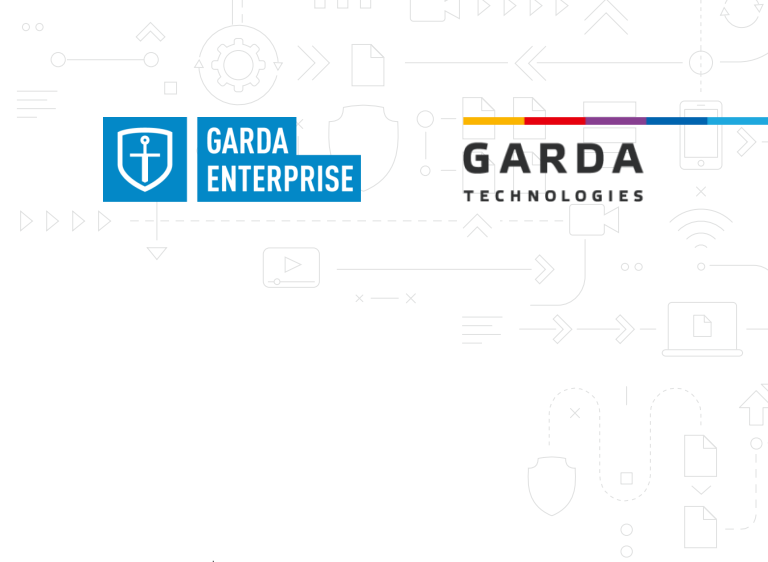


## Linguistic analysis

- Keyword and phrase-based searching for text data with due regard to morphology in text and graphic files (also in archives).
- Dictionaries help categorize intercept data by subject



# CORPORATE SECURITY



## CUTTING-EDGE TECHNOLOGIES THAT HELPED US CREATE GARDA ENTERPRISE EXPAND DLP END-USES



### EFFICIENT DATA LEAK PROTECTION

Exploiting proprietary high-precision confidential data identification algorithms, Garda Enterprise protects data across all communications channels and immediately detects security policy violations.



### SMART ANALYSIS SYSTEM

Analyzes trends of the corporate data streams, which allows for establishing a long-term response strategy and identifying suspicious activity in real time.



### HANDY CONTROL TOOL

Interactive security policy creation, controlling staff access to data resources, devices, and documents. Work time efficiency control.

# SYSTEM MANAGEMENT



## GARDA ENTERPRISE'S INTUITIVE WEB INTERFACE IS ADAPTED TO THE USER'S ROUTINE



Simplicity and user-friendliness



Superior performance



Cross-platform interface supporting any device and operating system






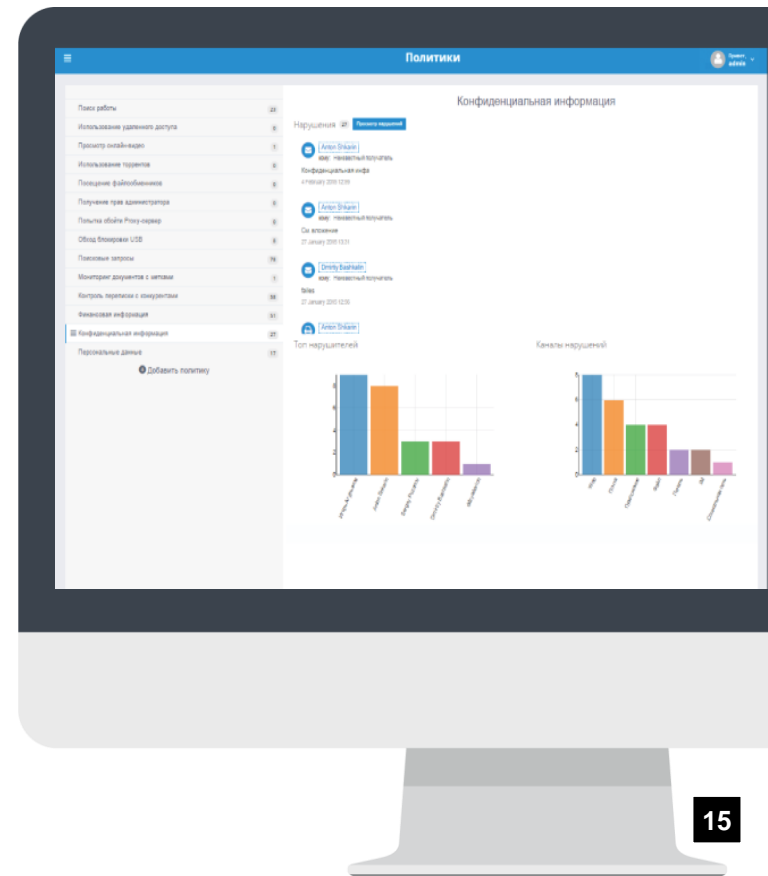
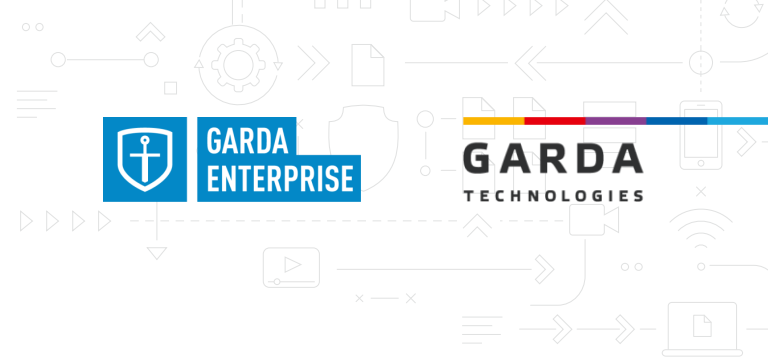
Main page can be flexibly tailored to everyday activities



# SECURITY POLICIES

## INTERACTIVE POLICY CREATION WITH RESULT ASSESSMENT

-  Immediate policy result after creation — edit policies in real time to achieve the intended result, clearly and quickly.
-  The system allows designing policies of any complexity with the use of diverse criteria (data type, software, communications channel, etc.) and specifications (keywords, labels, search criteria and their combinations).
-  The system will notify you of security policy violations via email.

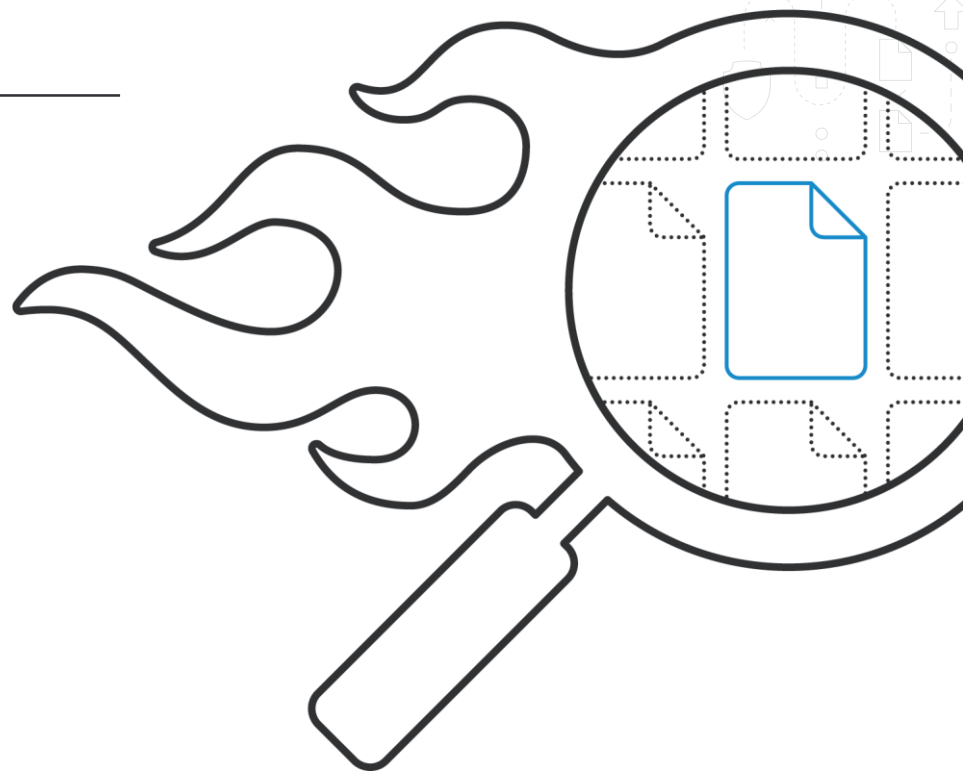


# ULTRA-FAST SEARCH



## SEARCHING THE OBJECT BASE IS AS EASY AS USING POPULAR SEARCH ENGINES

- Objects found are presented in a reading-friendly form. The user can apply diverse search criteria.
- Search any file types and archives.
- Search templates can be saved. Regular scanning. Get event notifications without including them into the policy list.
- The system stores the full copy of all communications. If new rules and policies appear, you can perform a retrospective analysis through the archive (such data would be lost forever in another system).





# SEARCH CRITERIA

- Keywords and phrases (also in attachments and archives), including images and scanned documents
- Searching for similar documents
- Searching regular expressions
- User's domain account in Active Directory (importing staff data from authentication server LDAP)
- Analysis criteria:
  - Ready regular expressions
  - Ready dictionaries and website lists

- File name, document property, type, size, etc.
- IP, protocol, port
- IM service ID (Skype, ICQ, MSN, etc.)
- Social network user ID
- Email
- VoIP – login/phone



Search any file types and archives



Retrospective data search by parameters



Ultra-fast search through all data



# BIG DATA HANDLING



## Data stream monitoring and control:



- A traffic analyzer checks whether data transmitted along network channels conform to data security policies.
- A workplace agent controls the computer and connected peripherals, ensuring the execution of data security policies.

## Integrated control center:



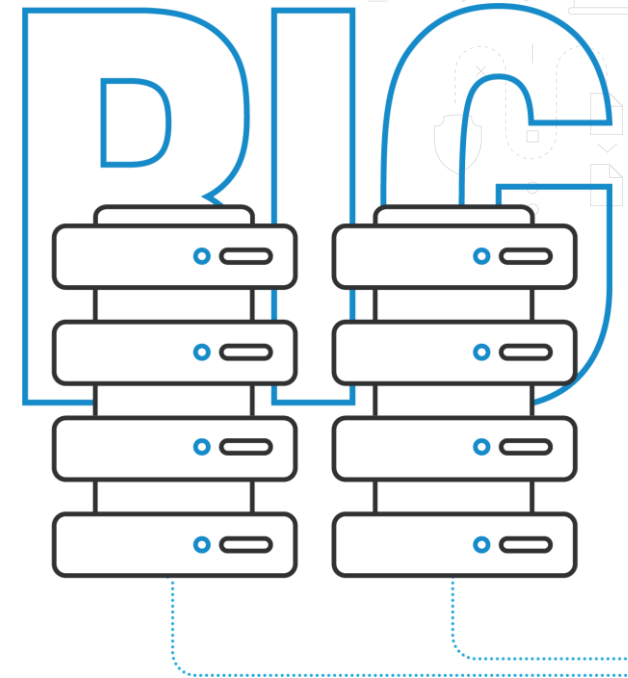
Administration and control of all system components, including managing workplace agents, creating data security policies, carrying out investigations, managing the data archive. The system automatically analyzes data to identify data security policy violations and anomalies, and generates reports.

## High storage and search performance:



Preserving its performance, the system ensures storage of data related to data security incidents and allows for recording and storing all data exchanged within the company.

Regardless of whether users work in the system, data are continuously monitored and captured across all communications channels.



# TRAFFIC DECODING



CONTROL ALL DATA TRANSMISSION CHANNELS OVER THE FOLLOWING PROTOCOLS:

## EMAIL AND NEWS PROTOCOLS



SMTP; SMTPs; IMAP4; POP3; POP3s; MAPI; NNTP; S/MIME: MS Exchange. HTTP, HTTPs (методы GET и POST) v 1.0, v 1.1. FTP, FTP over HTTP, tunneling (IP-in-IP, L2TP, PPTP, PPOE), Telnet, Authentication Protocol Kerberos 5.

## MESSENGERS



OSCAR (ICQ v7, v 8, v9); HTTPIM (social media messaging); MSNP v.12, v.13 (MSN Messenger, Windows Live Messenger); YMSG v9.0.0.2034 (Yahoo Messenger Protocol); IRC; MMP (Mail.Ru Agent); Skype; MS Lync; XMPP (Google Talk, Jabber QIP, SMS)..

## VOIP TELEPHONY



SIP v .2.0 (RFC 2543bis/3261); SDP, H.323 v .2; H.245 v .7; H.225 v .4; T.38; Megaco/H248; MGCP, SKINNY; H.263 ABC; H.264 (single NAL unit mode), including video telephony. Each VoIP telephony session may be presented as a full dialog or separate channels (incoming or outgoing).

## FILE EXCHANGERS



BitTorrent (standard 11031); Gnutella (v0.6); E-Mule (v0.49b); Direct Connect Protocol (dc++ v0.707).

# ENCRYPTED TRAFFIC AND CONNECTION BLOCKING

ENCRYPTED CONNECTIONS ARE DECODED BY A MODULE INSTALLED IN THE GAP OF THE NETWORK TRAFFIC



- The system intercepts and accumulates data across all communications channels
- Identifies an incident reason thereby allowing for the retrospective analysis of employee actions
- Immediate incident registration (also based on previously accumulated data), providing extensive visualization capabilities (diagrams and reports)



## HOW IT WORKS

The encrypted message selection module blocks HTTP and HTTPS connections to the preset resource list (by URL). For instance, it blocks access to social media or cloud drives.



## KEY CAPABILITIES:

- Immediate extraction of encrypted connection data
- Uploading external SSL certificates
- Bypass adapter for higher fail-safety



# FILE TRANSFER BLOCKING

OWN FILE LABELING TECHNOLOGY  
HELPS BLOCK CONFIDENTIAL  
DOCUMENT TRANSFER AND TRACK  
IMPORTANT DATA

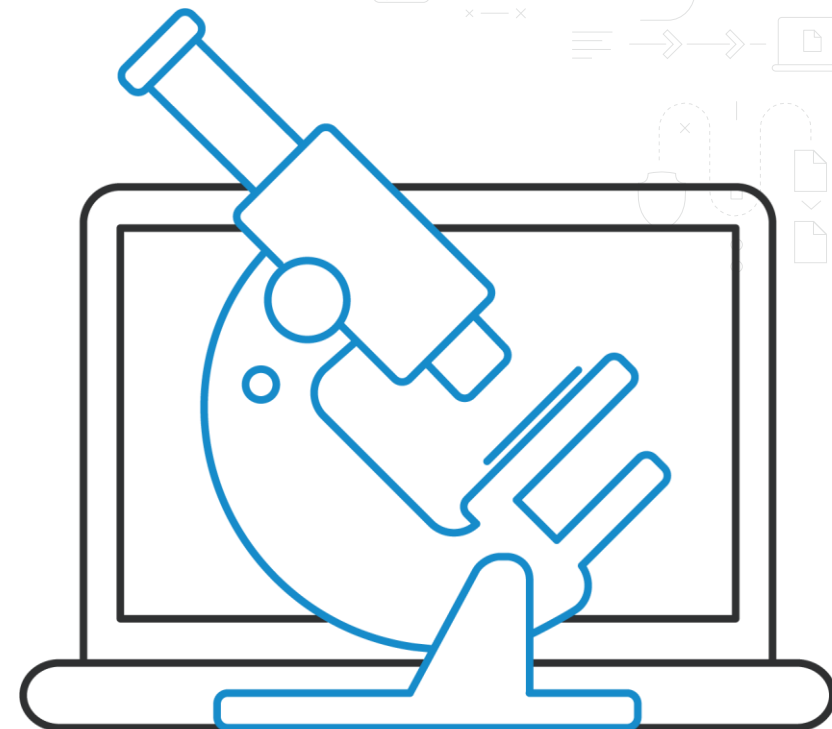


# ANALYTICAL CAPABILITIES

ONE-OF-A-KIND REPORTING SYSTEM ALLOWS CONTROLLING SECURITY POLICY COMPLIANCE, FORECASTING DATA LEAKS, AND IDENTIFYING ANOMALIES IN THE DATA ENVIRONMENT



The system controls security policy compliance, forecasts data leak channels, and identifies behavioral deviations.



# ANALYTICAL CAPABILITIES



## INTERACTIVITY

Analytics presented in graphic reports is interactive: you can go to any object (message, webpage, messenger chat, etc.)



## REAL TIME

All reports are generated in real time. When creating interactive data exchange routes and connections between employees, just drag a needed object into the report field, and the system will do the rest.



## BIG DATA HANDLING

Extensive analytical capabilities. The system provides statistical reports and specialized reports beneficial for incident investigation.



Beside security analysis, the system allows controlling staff work time, identifying cases of improper use of work time.

# ANALYSIS TECHNOLOGIES

## GARDA ENTERPRISE FEATURES THE MOST EFFICIENT ANALYSIS SOLUTIONS

### SEARCHING FOR SIMILAR DOCUMENTS



Helps find documents and document fragments in data transferred by users. Identifies unauthorized data access and distribution.

### LINGUISTIC ANALYSIS



Linguistic analysis algorithms help easily and efficiently find needed information with the use of the built-in search engine. Such algorithms improve the efficiency of security policies.

### TEMPLATES (REGEXP)



Identification of structured data in a data stream (ID card numbers, card numbers, emails, etc.). Helps protect personal data and financial documents.

### OPTICAL CHARACTER RECOGNITION (OCR)



The system allows recognizing texts in images for further analysis. No special licensing required.



GARDA  
ENTERPRISE

GARDA  
TECHNOLOGIES



# SYSTEM MANAGEMENT

GARDA ENTERPRISE'S WEB INTERFACE WAS DESIGNED WITH DUE REGARD TO DATA SECURITY DEPARTMENT ACTIVITY FOR MAXIMUM PERFORMANCE AND CONVENIENCE

**Desktop:** data security status, latest incidents, anomalies, statistics by key parameters.

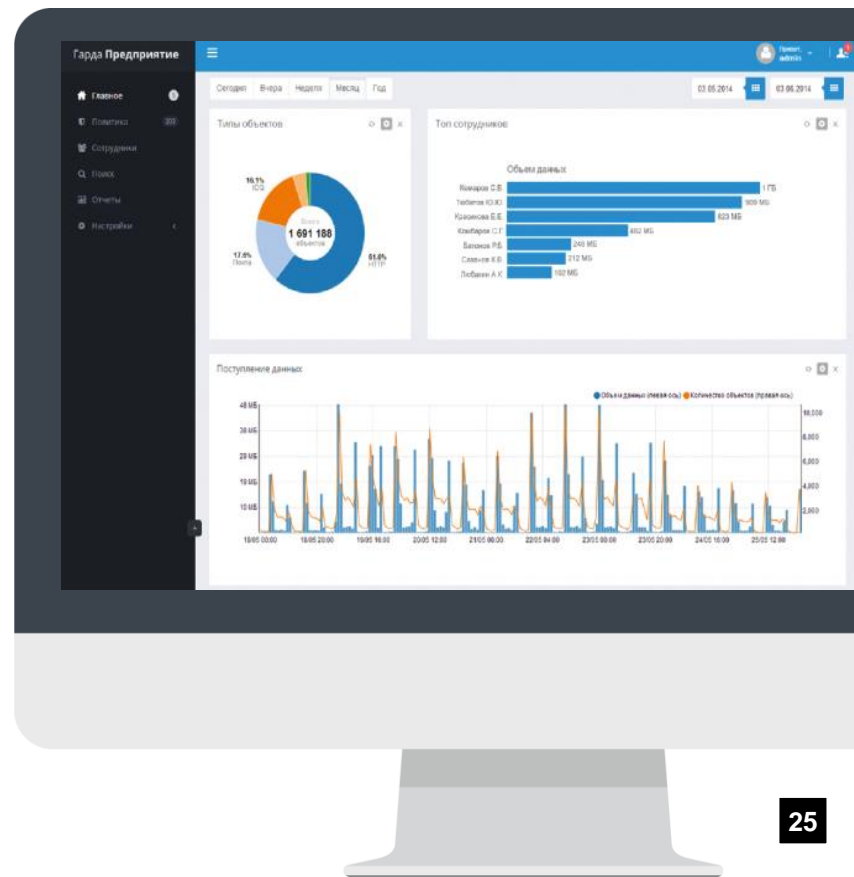
**Policies:** security policies.

**Employees:** employee list, personal cards, recent actions.

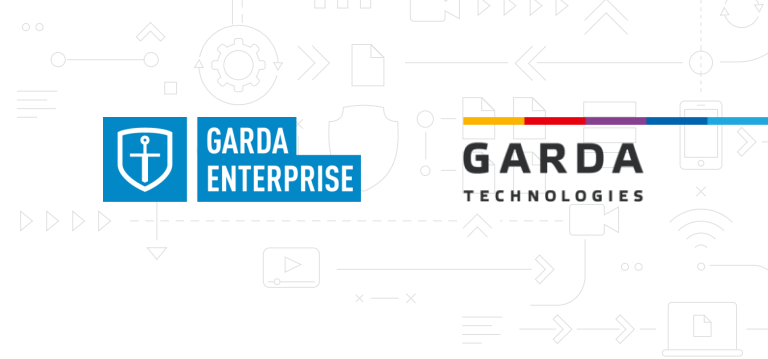
**Search:** searching for various objects in intercepted data (messages, documents, visited pages, etc.), grouping such objects, creating policies based on search queries.

**Reports:** multilevel graphical reports with statistics on various parameters.

**Settings:** program settings, workplace agent management (including installation and removal).



# STATISTICAL REPORTS



## DRILL-DOWN REPORTS: SWITCHING FROM A GENERAL REPORT TO A DETAILED REPORT AND OBJECTS



Reports help identify trends and deviations in the statistics of data exchange between employees.



# STAFF RELATIONS

THIS INTERACTIVE REPORT VISUALIZES THE CLOUD OF AN EMPLOYEE'S COMMUNICATION WITHIN THE COMPANY AND WITH THE EXTERNAL ENVIRONMENT. REFLECTS THE COMMUNICATIONS INTENSITY AND DATA TRANSFER MEANS

## DATA VISUALIZATION



Search result visualization by identifier (channels, senders, recipients, etc.)



Interactive charts (drill down)







Context routing



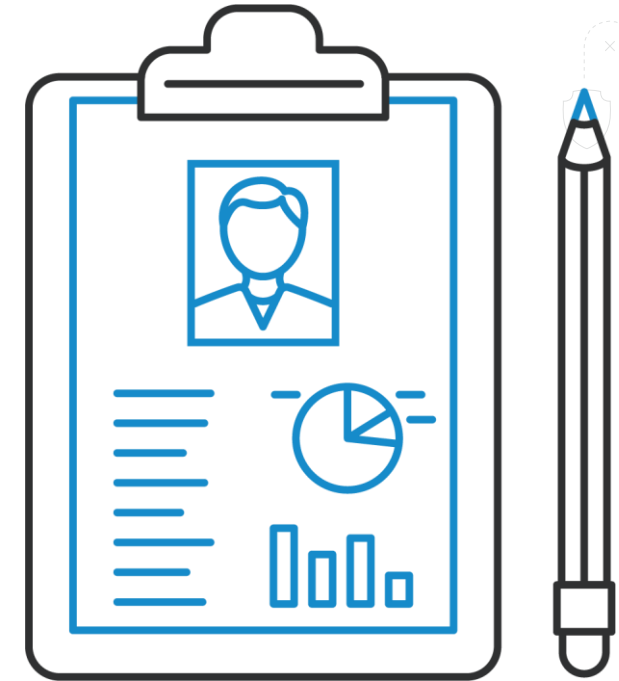
# EMPLOYEE CARD

SAVE TIME SPENT ON ROUTINE. GARDA ENTERPRISE AUTOMATICALLY FILLS EMPLOYEE PROFILES

SELECT AN EMPLOYEE TO SEE THEIR PROFILE

 Identity: title, photo, etc.	 Credentials
 Activity statistics	 Latest events

You can add data manually for more accurate monitoring of the employee's traffic.

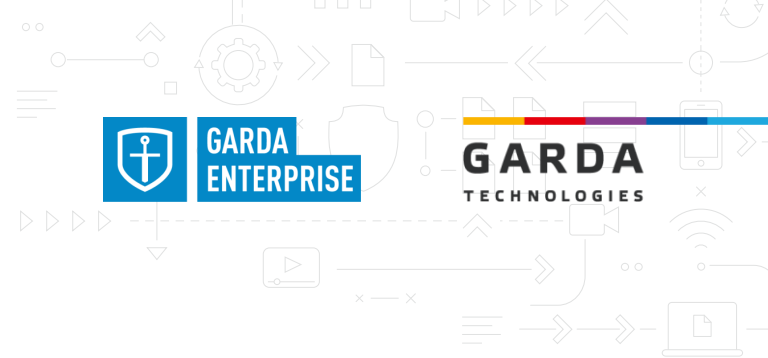


# CONTENT ROUTES

THIS REPORT VISUALIZES THE JOURNEY OF ANY PIECE OF DATA FROM THE FIRST COMMUNICATION TO TRANSFER OUTSIDE THE COMPANY. REFLECTS BOTH USERS AND DATA TRANSMISSION CHANNELS



Helps time-efficiently investigate incidents, identify conspiracies, and find unauthorized data owners before confidential data leave the company.

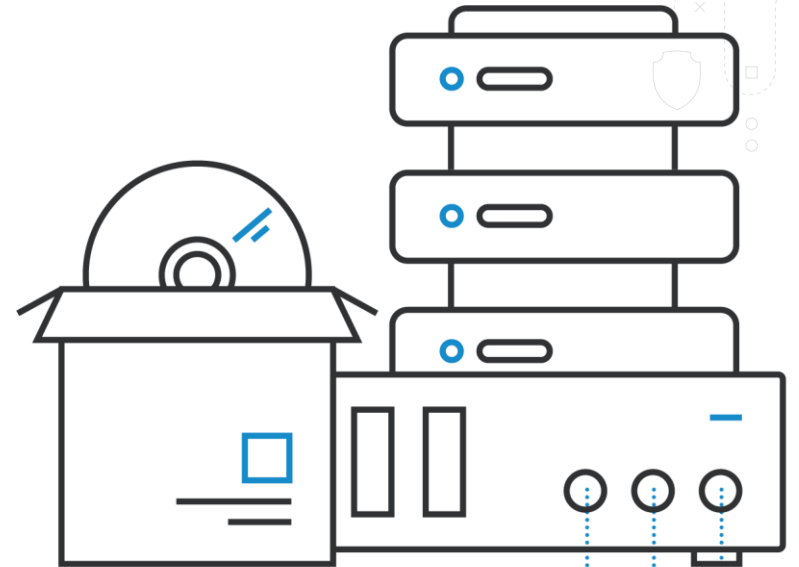


# SOFTWARE AND HARDWARE REQUIREMENTS

THIS SECTION REFLECTS SYSTEM FUNCTIONS, INCLUDING WORKPLACE AGENT MANAGEMENT, HTTPS HANDLING, TRAFFIC INTERCEPTION AND ANALYSIS, DATA STORAGE. PROVIDED ON A 1U/3U OR 4U SERVER (DEPENDING ON THE NUMBER OF WORKPLACES AND STORAGE PERIOD)



For instance, a standard solution for 400 workplaces and half-year data storage will be provided on a 1U server.



# END-TO-END SUPPORT

**GARDA TECHNOLOGIES  
ENSURES END-TO-END  
SUPPORT FOR  
IMPLEMENTING THE DLP  
SYSTEM INTO THE  
COMPANY  
INFRASTRUCTURE**



## **DATA RESOURCE AUDIT**

At the first stage, system specifications and data assets are analyzed. Based on analysis results, security policies tailored to the customer's needs are developed.



## **IMPLEMENTING DLP**

During the installation of a demo solution, the customer can see the efficiency of Garda Enterprise. Right from the box, the customer gets a wide range of security policies and reports. The system learns on real data for the first days—this ensures low fault triggering in the future.



## **SUPPORT**

After implementing and putting Garda Enterprise into operation, the technical support team helps the customer configure and adapt the system.



# 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



# THANK YOU FOR YOUR ATTENTION!



**GARDA**  
TECHNOLOGIES

info@gardatech.ru  
8 (831) 422 12 21  
**en.gardatech.ru**