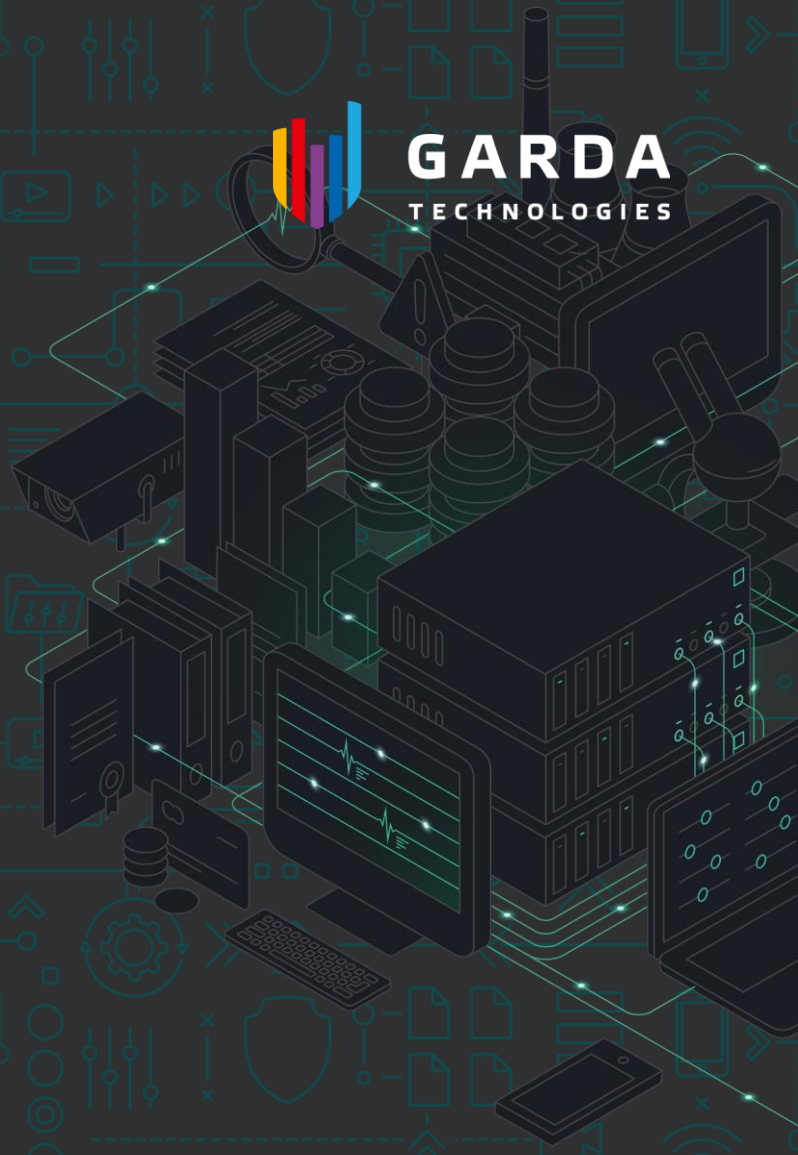
GARDA MONITOR

GARDA TECHNOLOGIES

GARDA MONITOR

NETWORK INCIDENT ANALYSIS AND INVESTIGATION SOLUTION



SYSTEM CLASSIFICATION

GARDA MONITOR

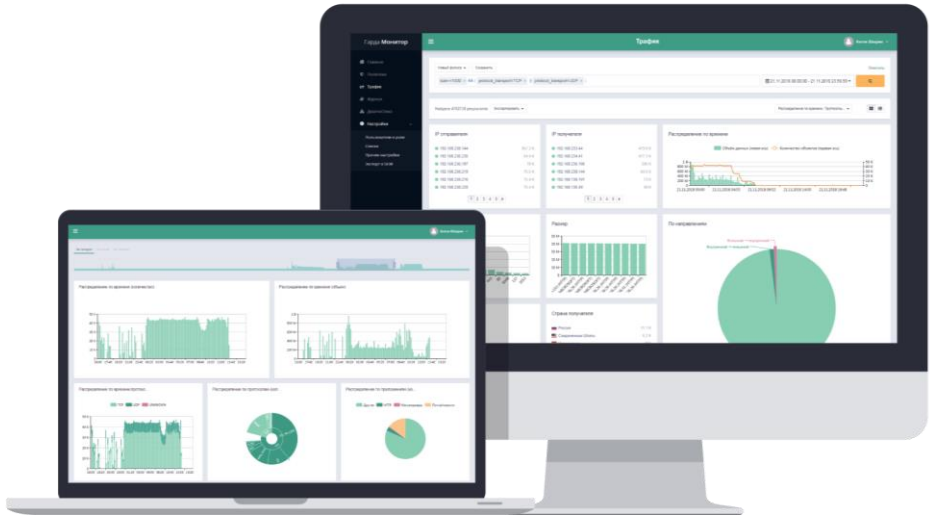
GARDA TECHNOLOGIES

NETWORK TRAFFIC ANALYSIS (NTA)

Network traffic analysis combines signature testing, machine learning, and advanced analytics to detect suspicious activity in the corporate network.

NETWORK FORENSICS

Measures aimed at identifying and investigating internal cybercrimes and fraud, and finding vulnerabilities in the corporate network infrastructure.



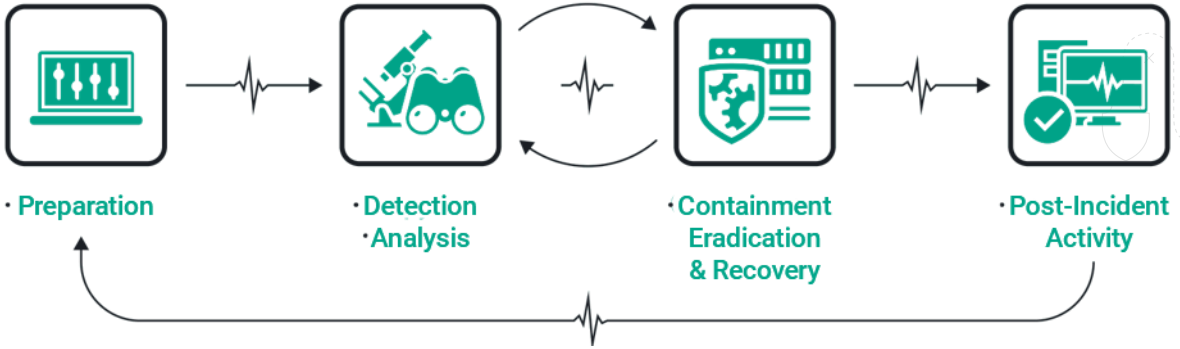
INCIDENT RESPONSE PROCEDURE

GARDA MONITOR

GARDA TECHNOLOGIES

INCIDENT RESPONSE PHASES *

*Pursuant to the Computer Security Incident Handling Guide NIST SP 800-61 R2



TRAFFIC CONTROL AND ANALYSIS

Local network IP traffic monitoring and network security incident identification

Keeping the archive of data exchange objects for the purposes of retrospective analysis

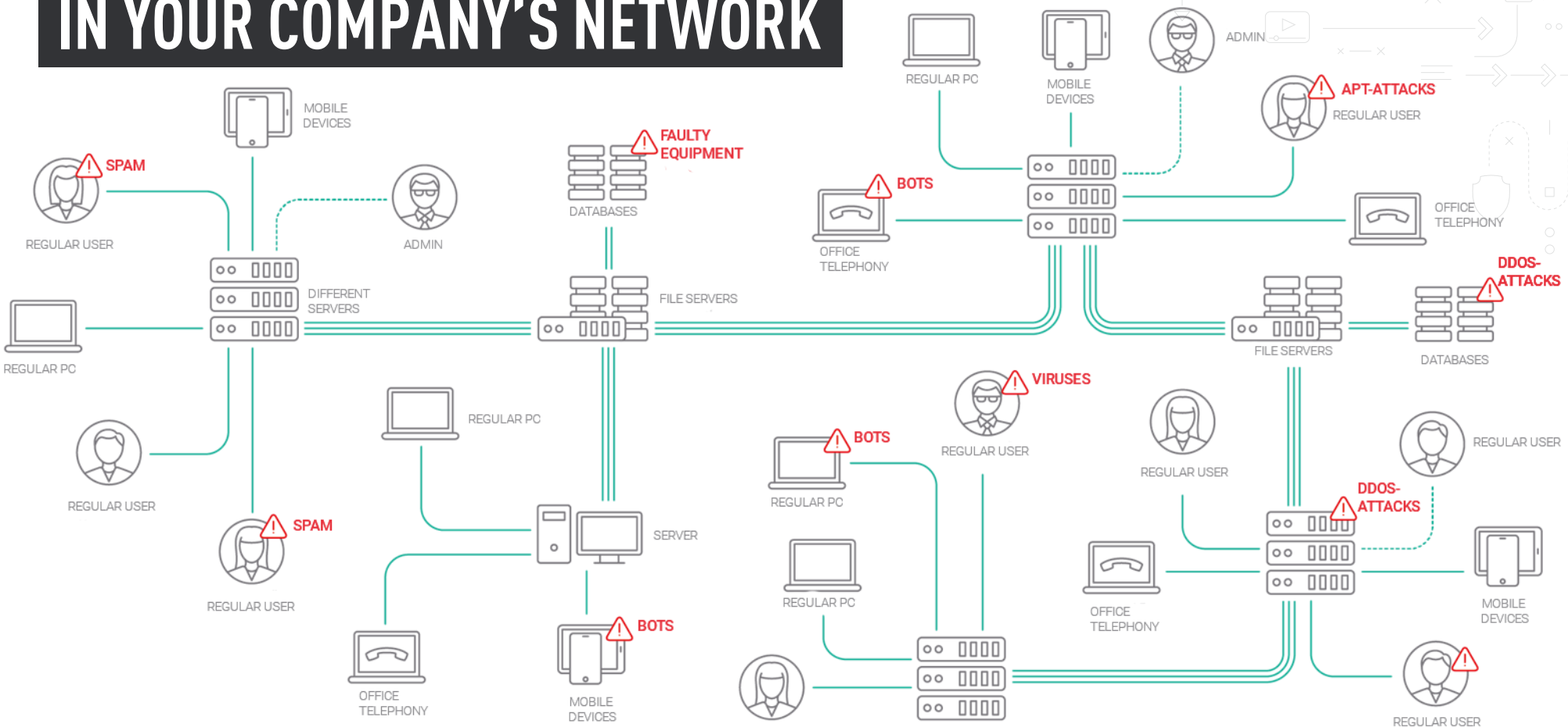
Behavior analysis: forming device profiles, identifying behavioral anomalies and significant deviations

Analyzing data streams over remote control, tunneling, online game, and other protocols

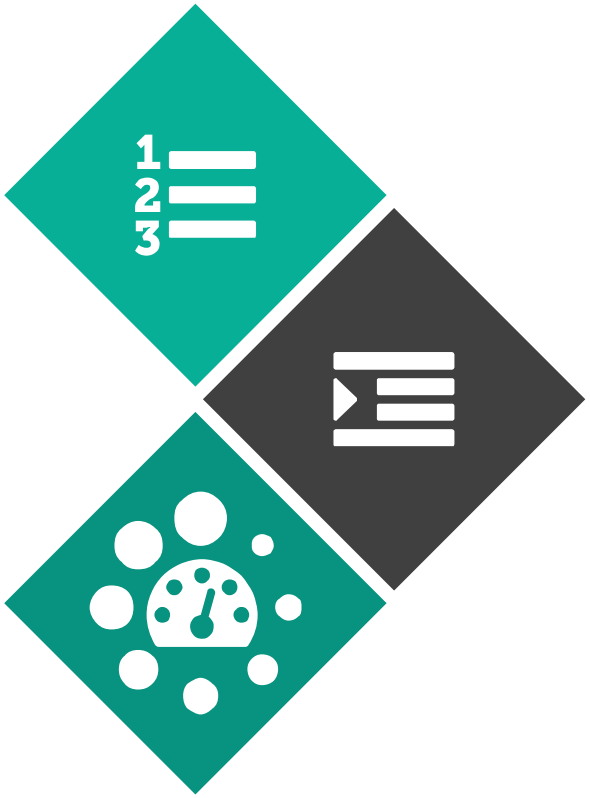
WHAT IS GOING ON IN YOUR COMPANY'S NETWORK

GARDA MONITOR

GARDA TECHNOLOGIES



NETWORK ANALYSIS COMMON PROBLEMS



TOO MANY STREAMS

Analyzing logs of each system is a time- and knowledge-intensive process
.

UNPROTECTED LOGS

The system admin can modify logs.

PEAK LOAD DURING AUDIT

Network activity audit increases the load on systems and devices.

FULL CONTROL OF NETWORK INFRASTRUCTURE

GARDA MONITOR

GARDA TECHNOLOGIES

GARDA MONITOR IS A SOLUTION DESIGNED FOR EFFICIENT NETWORK SECURITY ANALYSIS

STORAGE OF ALL L2-L7 LEVEL DATA

Recording enterprise traffic,
local network traffic, and Internet traffic.
Reproduction of any data stream.

DATA PACKETS AND STREAMS CLASSIFICATION

Traffic classification by protocol.
Locating data source and receiver.
Recording metadata.

IDENTIFYING ANOMALIES

Real-time anomaly identification,
namely network activity burst or decrease,
use of unusual ports, protocols, and apps.

GARDA MONITOR

GARDA TECHNOLOGIES

SYSTEM COMPONENTS AND THEIR PERFORMANCE

Forming a geographically-distributed cluster

Real-time handling of large lists

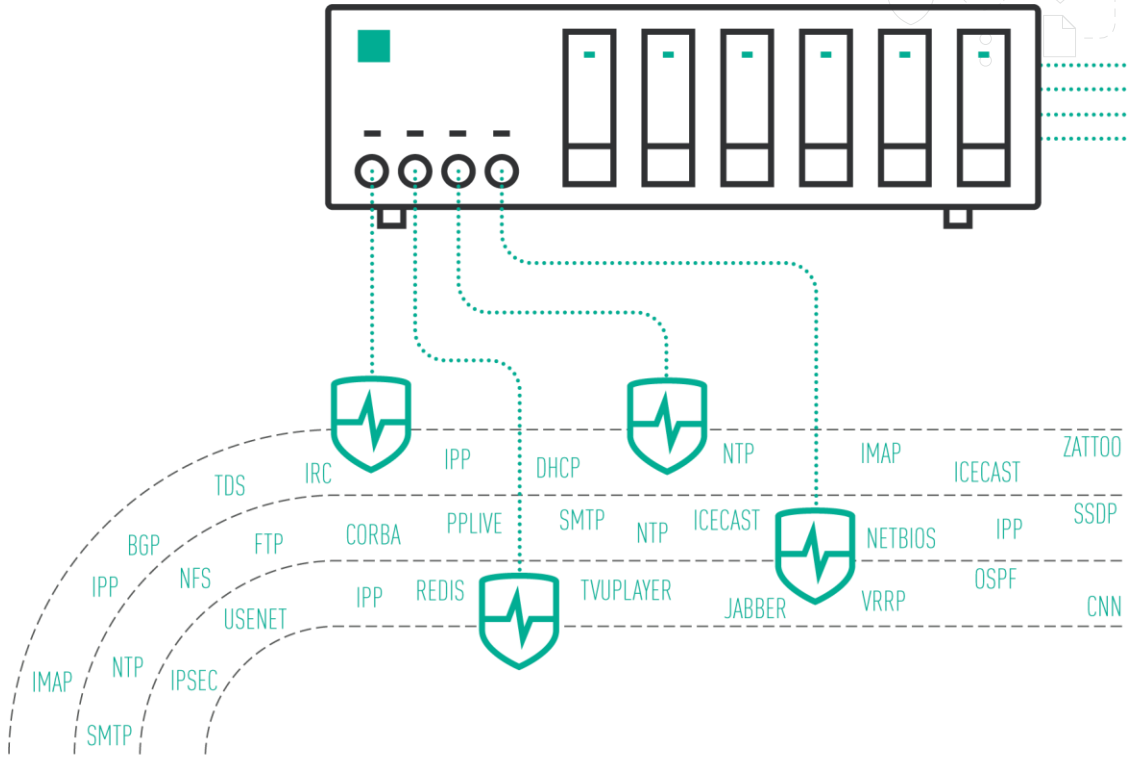
Flexible implementation: Netflow and traffic copy

1 DATA COLLECTION

→ 2

The system continuously captures and analyzes traffic in real time.

For distributed implementation circuits, all data are available in the single control center



SYSTEM COMPONENTS AND THEIR PERFORMANCE

GARDA MONITOR

GARDA TECHNOLOGIES

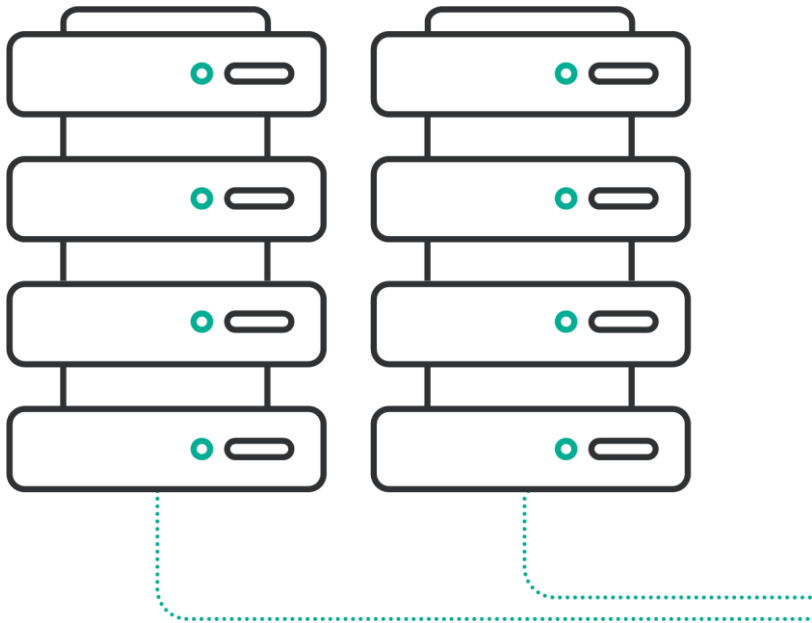
2 DATA STORAGE

1 ← → 3

Non-relational quick-access storage not requiring costly equipment or licenses is a proprietary DataWarehouse solution of Garda Technologies.

Cyclic incident re-recording.

Flexible recording settings configuration



SYSTEM COMPONENTS AND THEIR PERFORMANCE

GARDA MONITOR

GARDA TECHNOLOGIES

3 ANALYTICS AND MANAGEMENT

2

- Traffic conformity analysis
- Identifying suspicious events and incidents
- Intercept objects are displayed in a clear format
- Various report templates

DPI
DEEP PACKET INSPECTION

Network Forensics
Network Monitoring

EBA
ENTITY BEHAVIOR ANALYTICS

IDENTITY TRACKING

USE CASES

#1 1 MALICIOUS SOFTWARE:

- Abnormally high number of email messages sent from a computer (spam bot).
- Abnormally high number of DNS requests sent from a computer (Trojan or botnet).
- Identifying streams by IP from the black address database

#2 SUSPICIOUS USER ACTIVITY:

- Detecting facts of using software at workplaces: cloud storage queries, online games
- Detecting the use of DarkNet (Tor, I2P)
- Identifying suspicious services (unknown DBMS's, web servers within a network)

USE CASES

#3 SUSPICIOUS INTERACTION WITH EXTERNAL NETWORKS:

- Detecting attempts of remote access from external networks from other countries to internal servers
- Identifying VPN channels to addresses in foreign countries

What makes Garda Monitor special is that network stream data are stored separately from devices generating such streams.

This eliminates the chance of user interference aimed at deleting or deceiving data.

#4 STREAM LOGGING BY TIME:

Garda Monitor not only helps identify streams but logs their content in a time-based manner.

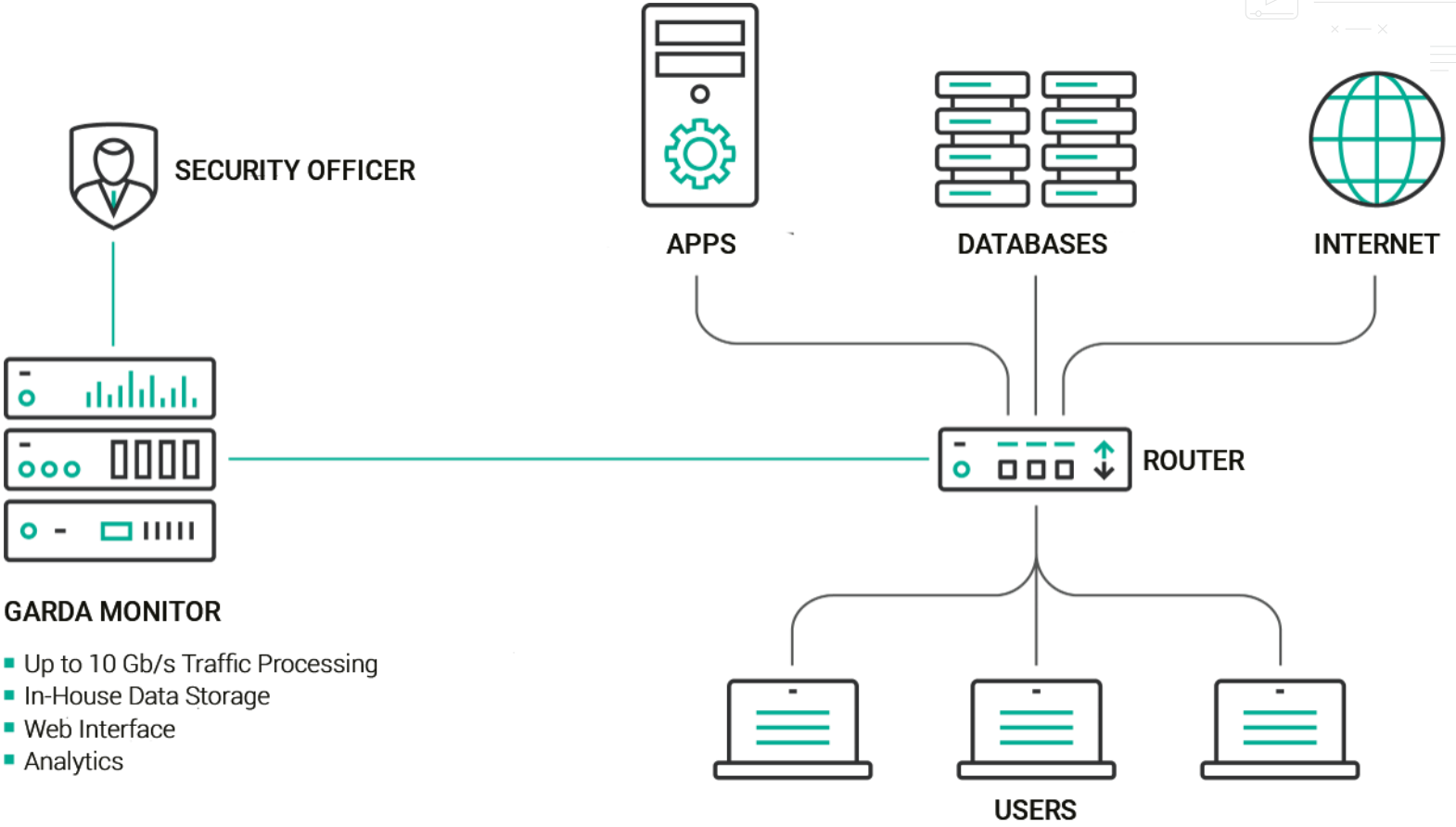
This allows:

- Exporting data for further detailed analysis
- Using those streams as evidence in the investigation and legal action.

IMPLEMENTATION CIRCUIT

GARDA MONITOR

GARDA TECHNOLOGIES



GARDA MONITOR

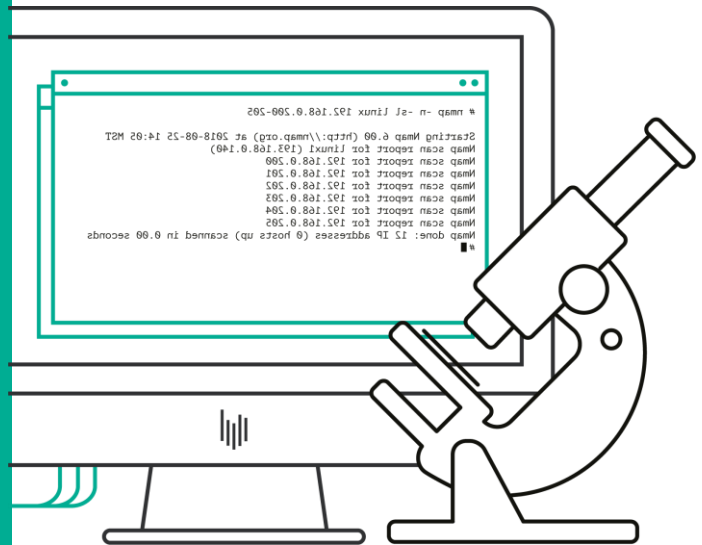
- Up to 10 Gb/s Traffic Processing
- In-House Data Storage
- Web Interface
- Analytics

EXTERIOR PERIMETER CONTROL & DS THREAT IDENTIFICATION

DoS-атаки (SYN-flood, ICMP-flood)

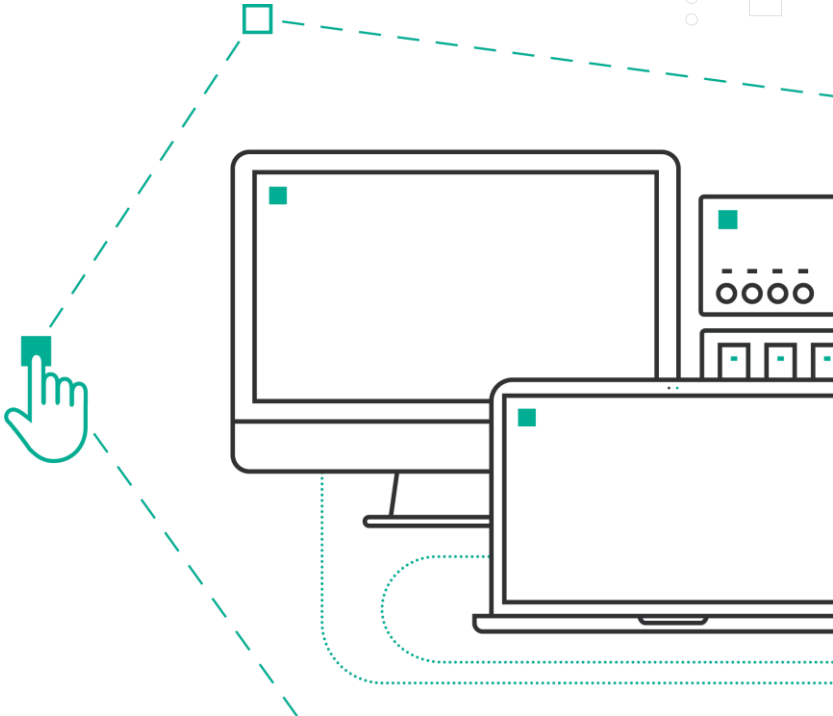
Post scanning

Host scanning



Detecting connections to points beyond the exterior perimeter from outside

Designating exterior perimeter points



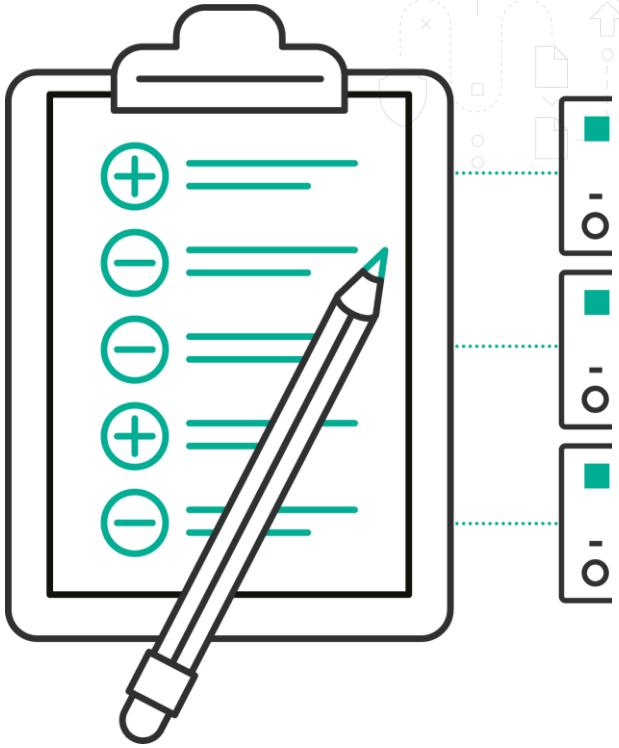
POLICIES

GARDA MONITOR

GARDA TECHNOLOGIES

EXTENSIVE LIST OF CLEAR AND HANDY POLICY TEMPLATES

- Query from and to a compromised IP
- Query to a compromised Host/URL
- Attempt of a DNS resolution of a compromised Host
- Using TOR, VPN
- Using remote access software ПО
- Off-duty traffic (games, app stores)
- FinCERT recommendations
- Web intelligence facts



ANALYTICS & RAPID SEARCH THROUGH INTERCEPT DATA

GARDA MONITOR

GARDA TECHNOLOGIES

ANALYTICS

REPORT PANEL INSTRUMENTS

Expert relationship analysis tools (visualization, infographics, graphs, etc.)

ENTITY BEHAVIOR ANALYTICS (EBA)

Forming device profiles, identifying behavioral anomalies and significant deviations

SEARCH FILTERS:

- ☑ Source/receiver MAC addresses
- ☑ Source/receiver IP addresses
- ☑ Source/receiver port
- ☑ Source/receiver account
- ☑ Source/receiver domain names
- ☑ IP protocol version
- ☑ Transport level protocol type
- ☑ Application protocol type
- ☑ Source/receiver country
- ☑ Transferred data volume

SIGNATURE TESTING

UPDATING

Automatic updating (no signatures, no rules).

CONTROL INTERFACE

Applying signatures and rules to the entire system infrastructure through the single control interface.

SIGNATURE BASES

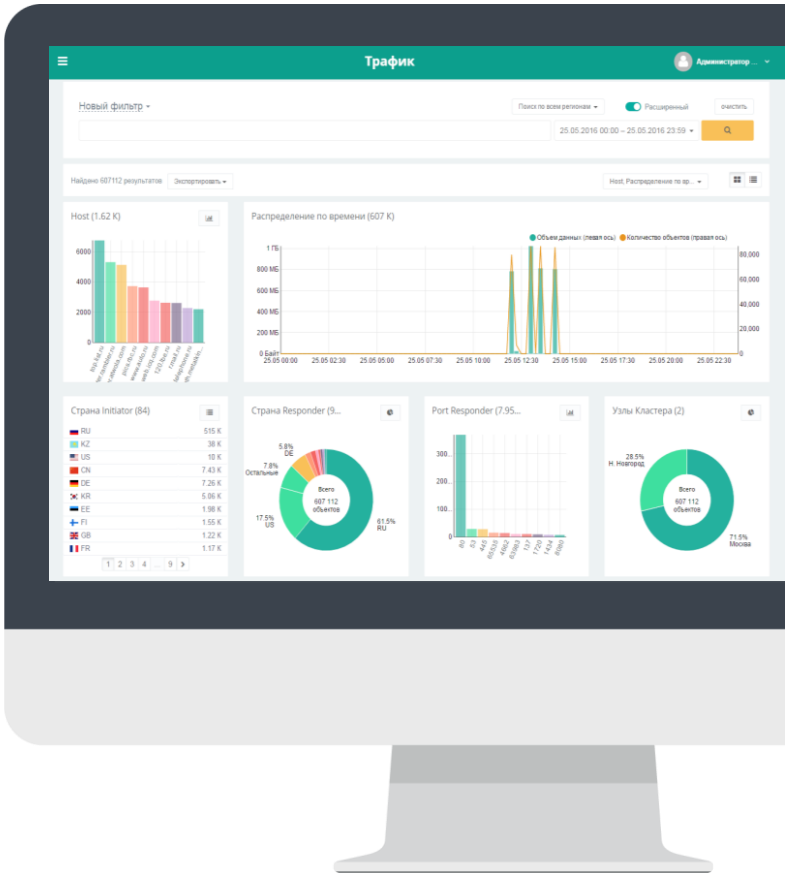
The system already contains connected and updatable signature bases.

REPORT EDITOR

GARDA MONITOR

GARDA TECHNOLOGIES

DIVERSE REAL-TIME REPORTS FOR UPPER-LEVEL NETWORK ACTIVITY ANALYSIS



REPORTS AVAILABLE:

- Graphical statistical reports
- Report templates
- Report generation based on data and time range

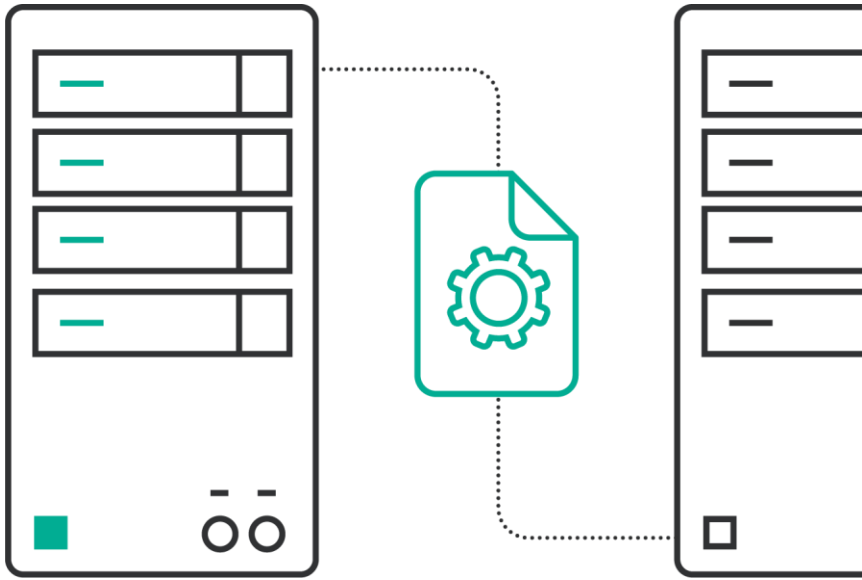
INTEGRATION, IMPORT & EXPORT

GARDA MONITOR

GARDA TECHNOLOGIES

AVAILABLE FORMATS	☑ CSV ☑ XML ☑ PDF ☑ SysLog ☑ Email
INTERNATIONAL BASES	☑ IP reputation bases ☑ Compromised website bases ☑ Compromised email bases (spam, phishing)

VARIOUS EXPORT/IMPORT FORMATS FOR INTEGRATION WITH SIEM SYSTEMS AND INTERNATIONAL DATABASES



SUPPORTED PROTOCOLS #1

GARDA MONITOR

GARDA TECHNOLOGIES

DATA TRANSMISSION

- HTTPS
- HTTP
- WAP
- FTP
- TFTP
- SMB
- BitTorent
- Filetopia
- iMESH
- OpenFT
- Kazaa/Fasttrack
- eDonkey
- DirectConnect
- AppleJuice
- PANDO
- StealthNet
- AFP (Apple Filing Protocol, AppleShare)

MESSAGING

- OSCAR (ICQ v7, v8, v9)
- IRC (Согласно RFC 2810-2813)
- MMP (Mail.Ru Агент)
- XMPP (QIP, Jabber)
- Tencent (QQ)
- MSN
- Yahoo
- MEEBO
- Skype
- WhatsApp
- Viber

AUTHORIZATION

- RADIUS
- TACACS+
- Diameter
- Kerberos

DATABASES

- PostgreSQL
- MySQL
- TDS
- MSSQL
- ORACLE
- Redis

NETWORK SERVICES

- RTP
- RTCP
- DNS
- SNMP
- SSH
- RDP
- RFB (VNC)
- NNTP
- MGCP
- TOR
- Opera Mini

PRIVATE NETWORKS

- OpenVPN
- CiscoVPN
- HotspotShield VPN

SUPPORTED PROTOCOLS #2

GARDA MONITOR

GARDA TECHNOLOGIES

EMAIL PROTOCOLS

- SMTP
- IMAP4
- POP3
- NNTP
- MS Exchange (MAPI)

GAMES & ENTERTAINMENT

- XBOX
- Steam
- Battlefield
- Quake
- Halflife2
- World of Warcraft
- WARCRAFT3
- Stracraft
- Armagetron
- World of Kung Fu
- Guildwars
- Florensia
- Dofus
- CrossFire

REMOTE CONTROL

- SSH
- TeamViewer
- RDP
- VNC
- PCAnywhere

MULTIMEDIA

- RealMedia
- Windowsmedia
- Icecast
- PPLive
- PPStream
- Zattoo
- SHOUTCast
- SopCast
- TVAnts
- TVUplayer
- VeohTV
- QQLive
- GloboTV
- Deezer

VOIP

- SIP
- Megaco (H.248)
- H.323
- SCCP (SKINNY)
- MGCP
- IAX
- WhatsApp Voice
- Webex
- TeamSpeak

SUPPORTED PROTOCOLS #3

GARDA MONITOR

GARDA TECHNOLOGIES

OTHER

- 99Taxi
- Aimini
- Apple (iMessage, FaceTime…)
- Apple iCloud
- Apple iTunes
- AVI
- BGP
- Citrix
- CitrixOnline & GotoMeeting
- CNN
- Collectd
- Corba
- DCE RPC
- DHCP
- DHCPv6
- DirectDownloadLink
- DNS
- DropBox
- EGP
- FaceBook
- Feidian
- Fiesta
- Flash
- GaduGadu
- Gmail
- Gnutella
- Google
- Google Maps
- GRE
- GTP
- I23V5
- ICMP
- ICMPv6
- IGMP
- Instagram
- IPP
- IPSEC
- KakaoTalk Voice and Chat
- Kontiki
- LDAP
- LLMNR
- LotusNotes
- MapleStory
- MDNS
- Microsoft Cloud Services
- MMS
- MOVE
- MPEG
- NETBIOS
- Netflix
- NetFlow_IPFIX
- NFS
- NOE
- NTP
- OFF
- OGG
- OpenSignal
- OSPF
- Popo
- PPTP
- QUIC
- QuickTime
- RemoteScan
- RSYNC
- RTCP
- RTP
- RTSP
- SAP
- SCTP
- sFlow
- Simet
- Snapchat
- SNMP
- Socrates
- Soulseek
- Spotify
- SSDP
- SSL
- STUN
- Syslog
- Telnet
- Teredo
- Thunder Webthunder
- TOR
- Truphone
- Tuenti
- Twitch
- Twitter
- UbuntuONE
- UPnP
- USENET
- VMware
- VRRP
- Whois-DAS
- Wikipedia
- WindowsUpdate
- WinMX
- XDMCP
- YouTube
- ZeroMQ

THANK YOU
FOR YOUR ATTENTION!

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