infocom
TRUSTED SECURITY

JE Infocom
8, Volodymyrska str.
Kyiv, 01001, Ukraine
tel.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoGuard

Multi-layered Network Perimeter Protection

infocom.ua

2024

INFORMATION SECURITY

The operation of a government or financial institution, a large or small business, an educational or medical facility is inseparable from the use of digital information technologies. These technologies significantly simplify, streamline, and automate processes, greatly enhancing the efficiency of organizational, financial, manufacturing, or other operations. However, unauthorized interference in the operation of your information infrastructure by malicious actors or unethical competitors can not only disrupt critical workflows but also lead to significant reputational and financial losses due to the leakage of confidential information.

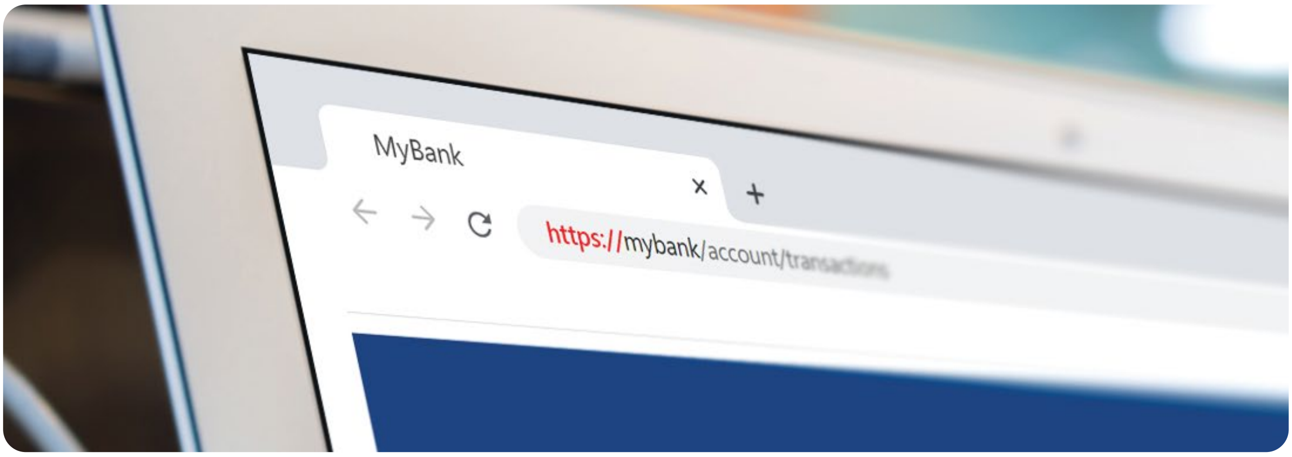
Infocom's information security services are designed to minimize any risks of unauthorized access to your infrastructure and ensure its reliable and continuous operation by providing comprehensive protection for both external and internal perimeters.

infoGuard

Web Page

MULTI-LAYERED NETWORK PERIMETER PROTECTION

infoGuard is the first line of defense for your information infrastructure. It is a critical component that prevents unauthorized external intrusions into the corporate network, monitors and tracks employee activities, and allows, denies, or terminates external access while enabling you to remain flexible and dynamic in achieving your business goals.



The extensive use of the secure HTTPS data transfer protocol, which makes it impossible to "eavesdrop" on network connections while visiting web pages of various online services, significantly reduces the risk of third parties intercepting private and confidential information. However, it simultaneously conceals the entire data stream between the user and the web portal from standard protection systems. This not only allows viruses, spyware, system monitors, keyloggers, and other malware to infiltrate the corporate network through employee computers but also hides outgoing data streams, which may contain sensitive corporate information.
Since, according to statistics, HTTPS traffic accounts for over 80% of the total, analyzing encrypted data has become one of the main components of modern information protection. The infoGuard

service enables encrypted data inspection by acting as an intermediary between users and web portals. This significantly reduces the risk of malware infiltrating the corporate network by analyzing all incoming and outgoing traffic without exception.

- The main goal of modern cybercriminals is to steal confidential corporate and personal information by exploiting vulnerabilities in installed equipment and software. The infoGuard Intrusion Prevention System continuously analyzes all external requests, helping prevent potential attacks and their negative consequences. In addition to analyzing external requests, infoGuard has a flexible internal control system. By analyzing outgoing data, it significantly reduces the likelihood of confidential information leaks caused by unintentional or malicious employee actions.

- The infoGuard service includes a dynamic web filtering feature that operates in real time. It blocks employee access to compromised or intentionally created resources that criminals use to gain access to personal and corporate data or to download malicious software.

  If requested by the client, the system allows the creation of additional filters to block employee access to specific websites or entire categories of web resources, such as gambling, online movie streaming, adult content, and more.

- The infoGuard application control feature continuously classifies and evaluates the traffic of applications used by employees. The control system allows blocking or restricting access to risky applications or entire categories of applications. It optimizes bandwidth usage in your network by setting application priorities or completely blocking unwanted traffic. For example, infoGuard service can block video viewing or audio streaming on social media while still allowing access to posts and photos.

The deployment and connection of the infoGuard service depend on whether the client is already using Infocom services, such as infoSDWAN, infoVPN, or Internet access. In this case, the connection process takes minimal time, and all switching and configuration work takes place within Infocom, without requiring additional work or configuration on the client's side (except for installing infoGuard certificates on work computers for encrypted traffic analysis). If the client is not using the above-mentioned Infocom services a GRE tunnel is created on the client's side, directing all incoming traffic to infoGuard equipment located at Infocom. Alternatively, the client is provided with a dedicated set of equipment that is installed at each endpoint and checks traffic directly on the client's side.

As part of the infoGuard service, Infocom specialists can take over the management of client equipment if the client does not have their own information security team. This means that our team will provide effective monitoring and protection of your networks and systems against malicious attacks and other threats, operating 24/7 using your equipment.

Benefits of infoGuard:

- Reduced risks of business disruption due to cyber threats.
- Cost optimization by eliminating the need for expensive equipment and licensing.
- Secure Internet usage.
- Flexible scaling of connected branches or departments, with options to increase or decrease connections as needed.
- 24/7/365 monitoring and incident management.
- Expert support from Infocom without the need for additional staff training.
- Round-the-clock technical support (24x7x365).