The infoGuard service can provide reliable protection of your infrastructure and data and will assist in compliance with all information security policies.

The main components of infoGuard service are:

- **Antivirus**

Traffic scanning provides protection against spyware and malware, including protection against trojans, phishing programs, system monitors, keyloggers, as well as protection against adware.

As more than 60% of network traffic is encrypted today, the ability to decrypt it and verify for threats is an essential element of modern security. InfoGuard offers this capability*, not only because this significant percentage of all corporate traffic needs to be verified, but also because it further enhances the effectiveness of key functions (for example control of bypass maneuvers, control and management of programs).

- **Advanced threat protection**

Our service includes several comprehensive modules for verifying sources of information regarding threats and options for protection against unknown threats, as well as monitoring the activity of client software.

infoGuard provides file analysis using an external cloud service (Sandbox), including the use of dynamic signatures for potential zero-day threats. Our service inspects SSL and TLS encrypted traffic with intrusion prevention profiles, provides application control, antivirus, web filtering, Botnet networks blocking using the world's largest reputation database and more.

* The client's PCs should have an infoGuard certificate.

- **Intrusion Prevention System (IPS)**

IPS provides protection through a vulnerability database and quantitative analysis. The prevention system is able to recognize and block TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding.

- **Application control**

Many programs have significantly different features that present different levels of risk to both the user and the organization.

The security system continually classifies and evaluates traffic, apps features, and monitors changes. Each time the behavior of an app is changed, the system checks it for compliance with the configured security policies.

Identifying and managing applications that share the same connection is an important feature because today the client works with many "platforms" (Google, Facebook, Microsoft, Salesforce, LinkedIn, or Yahoo) where application developers integrate many different programs that often have very different risk potentials and business value. For example, Gmail not only sends messages but also has the ability to create a Google Talk session right from the Gmail interface. These programs are fundamentally different, but our security system defines each one and applies a separate policy, according to the recommendations and wishes of the customer.

Software developers no longer adhere to the standard combination of ports and protocols; more and more applications are capable of running on non-standard ports (such as instant messaging programs, peer-to-peer file sharing, or VoIP). In addition, software developers are increasingly trying to get applications to work through non-standard ports (such as MS RDP, SSH). In this case, to ensure compliance with the specific rules, the security system classifies the program traffic (all the time on all ports), which allows flexible control of the rules of operation and behavior of each program.

Our solution also supports HTTP / 2 application traffic detection and the ability to block QUIC traffic so that the browser automatically returns to HTTP / 2 + TLS 1.2.

- **Content filter**

This feature includes dynamic, real-time web filtering with cloud-based web resource database with static filtering capabilities, secure search, such as transparent insertion of SafeSearch parameters into queries, support for Google, Yahoo !, Bing, YouTube Education Filter, etc. , creating local categories of web resources for the client's need, preventing proxy use, Java Applet filtering, ActiveX, cookies, blocking HTTP post actions, logging searches, rating images by URL, blocking HTTP redirects, setting quotas for browsing.

- **Data leakage prevention**

InfoGuard provides a high level of security with multi-level traffic filtering, which greatly reduces the likelihood of leakage of sensitive information! The service provides the ability to filter messages, files and has additional settings.

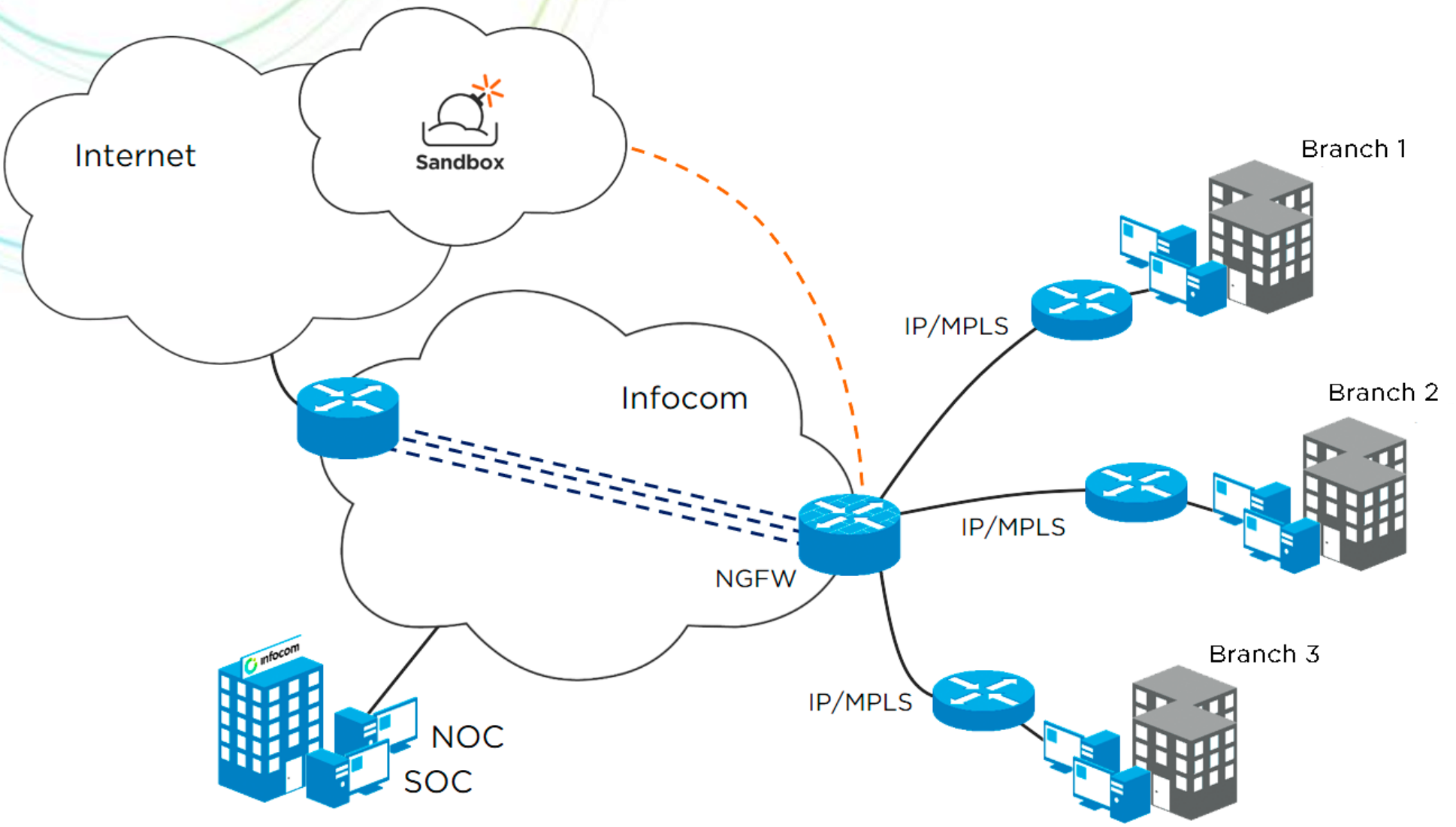
Message filtering (protocols):	HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP.
Files filtering (protocols):	HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP.
Filtering settings:	size, file type, watermark.

- **Workplace protection**

Workplaces are often the target of all kinds of cyberattacks. A recent study found that 30% of attacks were committed by installing malware at workplaces. By installing security agents with integrated means of tracking, by controlling and preventing the malware spread, we greatly enhance workplace security. Endpoint threat detection, monitoring, and assessment features help mitigate risks and reduce danger.

Service deployment

The infoGuard service can be launched both based on Infocom's own IP/MPLS network or based on other telecom operators' connections.



For all the equipment and software we use, we have **State Service of Special Communication and Information Protection of Ukraine** expert review regarding compliance with the requirements of regulatory documents of the system of technical protection of information in Ukraine.