infoMail

It is impossible to imagine a modern cybersecurity system without its integral component - Email protection. According to the Verizon 2019 Data Breach Investigations Report, **more than 92% of malware is received by Email**. Despite the security measures taken by companies, **49% of malware infections occur via Email**. Why is this happening? Modern cybercriminals use a variety of methods, but they are all usually based on the carelessness and inexperience of Email users. Using so-called social engineering, cybercriminals create special content targeted at users with the same interests, the organization, or individuals within the organization, content based on the interests or role of a particular user. They often create the illusion of "legitimacy" of the content, posing as the head of the company or representatives of partners, banks, etc., which leads to the leakage of confidential information of a private or corporate nature.

infoMail service is designed to withstand today's wide-spectrum threats posed by the use of e-mail such as viruses, malware, spam, Emails linking to resources containing malware, leakage of confidential information caused by phishing technologies, leakage of critical information caused by unauthorized nonintentional or intentional actions of the company's employees.

infocom

The infoMail service has the following components and properties

- **Antispam/Antifishing**
- **Antivirus**
- **Protection against new threats**
- **Protection against targeted attacks**
- **Analysis in the "sandbox"**
- **Compliance and data protection**
- **Management and reporting**
- **Flexible deployment**

Antispam/Antifishing

A simple, but at the same time, the fastest and most effective mechanism for protection against spam and phishing messages is the use of reputable databases. When you receive an email, the system checks the sender's IP address and content in a dedicated database. If the sender has a negative reputation, the letter is blocked. If there is no sender information in the database, the system performs additional analysis based on dynamic heuristics, header analysis, behavior analysis, and scans for malware. After verification, the sender is assigned a positive or negative rating, which is stored in the reputation database.

This technology allows you to effectively withstand mass spam/phishing attacks as the reputation base is constantly updated in real-time. Any new attack detected in one country is automatically blocked elsewhere.

- **Antivirus**

Modern protection is impossible without a reliable antivirus. The infoMail service has in its database **more than 50 000 signatures** of different variants of virus families. Like the reputation database, the virus signature database is constantly updated in real-time. During the scan, the antivirus analyzes the contents of attachments and, if necessary, unpacks existing archives, decrypts files, deletes the active content of suspicious files and HTML. If the system cannot identify the code as safe or unsafe, it performs a deeper analysis. This analysis is performed using a cloud "sandbox" where the code is emulated and its behavior is checked.

- **Protection against new threats**

To effectively withstand new cyber threats, the infoMail analytics center analyzes millions of emails per hour worldwide and can identify new dangerous code in minutes. All suspicious attachments found in emails are blocked for analysis in information security laboratories. The created database is constantly updated and is a common resource of **CYBER THREAT ALLIANCE**, which includes world leaders in cybersecurity.

CYBER THREAT ALLIANCE

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

FORTINET

paloalto NETWORKS

McAfee Together is power.

infocom

- **Protection against targeted attacks**

- link protection

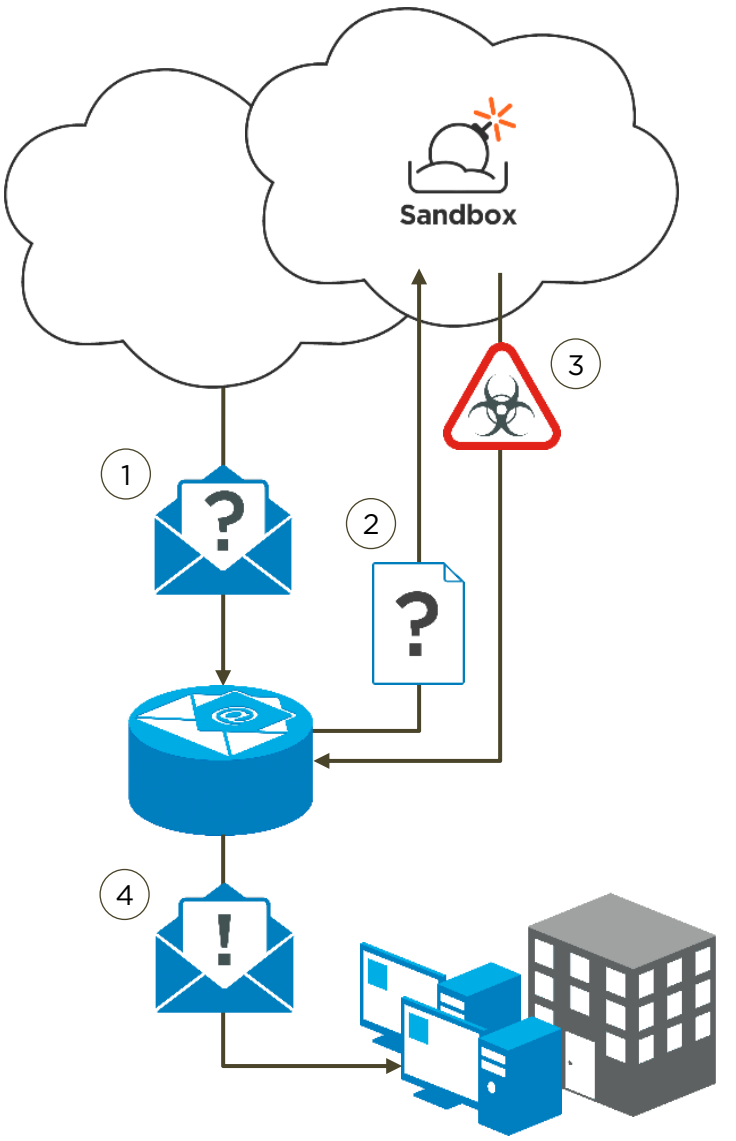
  The infoMail service uses effective tactics against criminals who, using social engineering, create messages with a link to a completely secure resource, and over time change the content of the resource to a malicious one. Typically, such messages are sent at night to have time to change the content of the site before the recipient reads the letter. Since the resource does not pose any threat during sending, the emails are easily checked by basic security systems. In turn, the infoMail Service makes a substitution of the original link and when the recipient tries to follow this link, it re-checks it for threats and only then gives access to the resource or blocks it.

- "disarmament" and content reconstruction

  The infoMail service automatically analyzes files and removes suspicious content such as macros, links, embedded objects (OLE, JavaScript, etc.). After deleting suspicious content, the file is reconstructed to look as close as possible to the original and sent to the user. The original file is quarantined and is available after a complete analysis based on the cloud security service. If the files are encrypted, the system can decrypt them using pre-loaded passwords or passwords found in the text of the email. If necessary, the service also allows categorical or selective removal of links from all received messages.

- **"Sandbox" - protection against zero-day threats**

The infoMail service checks emails and sends suspicious files and links to the cloud "sandbox" for further analysis. The "sandbox" creates a virtual environment in which suspicious code is run as if it got into the real system of the recipient. This check analyzes the actions of suspicious code, whether it tries to contact for instructions, whether it launches any processes that violate security policies, and so on. After verification, the system assigns an appropriate rating according to which further actions such as permission to deliver to the recipient or removal are performed.



- **Compliance and data protection**

Prevention of critical data loss is achieved by creating digital fingerprints of such files by manually loading into the system, or automatically scanning shared Windows folders. After that, the system analyzes all files sent for compliance with existing digital fingerprints and in case of security policy violation blocks their sending.

The system also has the ability to encrypt data using the TLS & S/MIME protocols and the authentication protocol, which does not require an additional license and does not exchange encryption keys

infocom

- **Management and reporting**

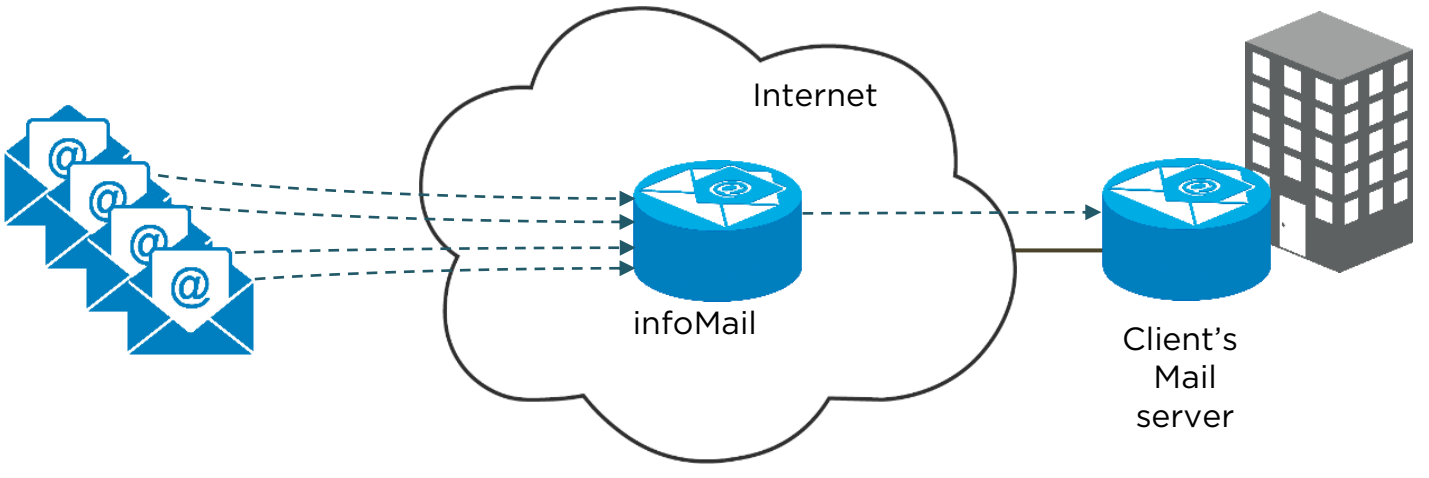
infoMail allows you to view the statistics of all users by providing comprehensive information on threats in real-time. The system allows you to cross-search events with millisecond accuracy in all available logs.

- **Flexible deployment**

The infoMail service can be deployed in both gateway mode and transparent mode. In gateway mode, all mail is sent to the infoMail server and, after verification, is forwarded to the client-server. This connection requires changes to client-server settings.

Gateway mode

Mail is delivered to infoMail, checked for threats and transmitted to the client's mail server.



In transparent mode, the Infocom equipment connects directly in front of the client's mail server. Transparent connection does not require any changes to the settings.

Transparent mode

Installed as a "wire insert". You do not need to change the server configuration.