KASPERSKY lab

Kaspersky Security Network

The Kaspersky Security Network (KSN) is a complex distributed infrastructure dedicated to processing depersonalized cybersecurity-related data streams from millions of voluntary participants around the world. It delivers Kaspersky Lab's security intelligence to every partner or customer via the Internet, ensuring the fastest reaction times and the maintenance of the highest levels of protection. It is one of the most important components of Kaspersky Lab's protection solutions.

Protection from unknown and advanced cyberthreats

According to Kaspersky Lab data, about 325,000 new malicious files are found "in the wild" every day and 113,500 phishing wildcards are added to the company's anti-phishing database every month. However, cybercrime has grown, not only in volume, but also in sophistication. Kaspersky Lab's internal stats show that just 70% of the threats faced by users every day are known ones, while 30% are unknown and advanced ones demanding additional layers of protection. That is why traditional signature-based protection is not enough, and all leading security vendors today use hybrid protection – a combination of device-based and cloud technologies.

This approach combines the advantages of traditional defensive methods, minimizing their shortcomings, with the potential of global monitoring and the continuous updating of information about new threats. The three main benefits of using this kind of cloud protection are:

- better detection rate
- reduced reaction time
- minimization of false positives

The basic principles of the Kaspersky Security Network

- KSN automatically analyses data received from all over the world in order to detect new cyberthreats better and faster and provide users with protection against them in a way that doesn't affect device usability;
- The information that is processed is received from customers who have agreed to participate in KSN – this feature can be opted out of or limited either at or after the installation of a Kaspersky Lab security solution[i];
- The data received by KSN does not contain information that is legally regarded as 'personal' by most countries, such as names, contact details or other credentials, and the data is not attributed to a specific person. The kind of information obtained is

described in full in the End-User License Agreements (EULA), which are available in the "Support" sections of local Kaspersky Lab web-sites.
- Kaspersky Lab protects this information in accordance with current statutory security requirements and to the highest industry standards;
- Data sent to a user's device from KSN is comprehensively encrypted and safe from Man-in-the-Middle attacks.

Kaspersky Security Network workflow

Kaspersky Security Network's working mechanism includes several key processes such as the continuous, geographically-distributed monitoring of real-life threats on users' computers, analysis of that data, and the delivery of relevant intelligence and countermeasures to protected endpoints. The information about infection attempts is analyzed using the company's powerful in-house expertise and technological resources.

The safety of a program is determined through several factors, including the availability of the vendor's digital signature and control hash, and verification of the source and integrity of the program. A website's safety is determined through checking the company's certificate and the analysis of webpage content.

Once a program or website is recognized as legitimate, it is added to the list of trustworthy applications or websites (the whitelisting database). As soon as a program or website is defined as malicious, it is reported to Kaspersky Lab's Urgent Detection System and the information is made available to all users through the Kaspersky Security Network.

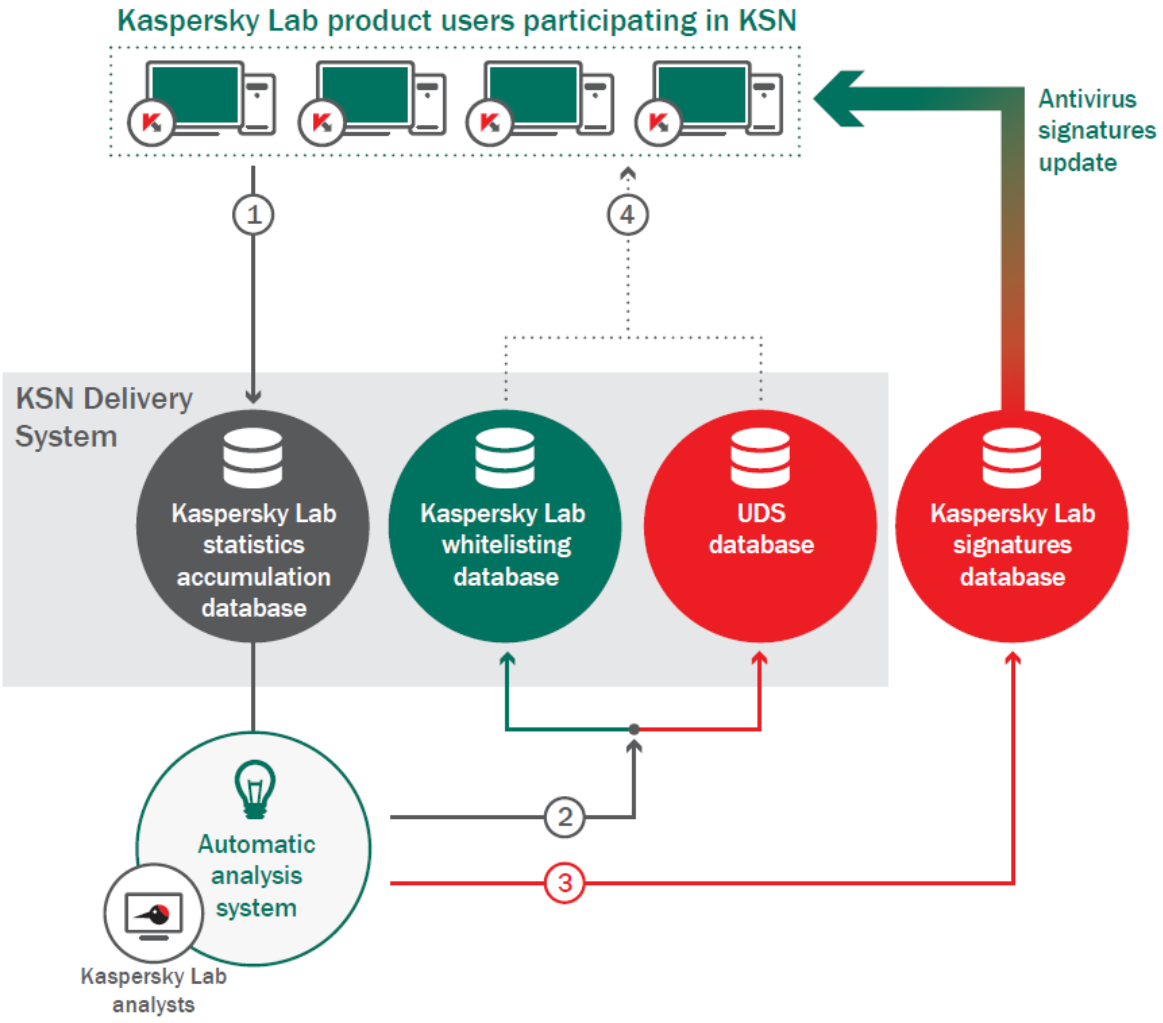
While creating and uploading the signature to a traditional signature database takes hours, with KSN users receive a corresponding measure of protection within minutes of the launch of a cyberattack. KSN therefore assists both signature-based and heuristic detection in addition to supporting whitelisting and application-control technologies via the continuous updating of the list of legitimate programs.

Another feature of KSN that is worth a separate mention is its cloud-assisted anti-spam technology. This uses information from the cloud to detect and block unsolicited messages so that users do not require a local anti-spam filter.

The flow-chart below illustrates the basic principles on which Kaspersky Lab's products interact with KSN. This interaction includes four different phases:

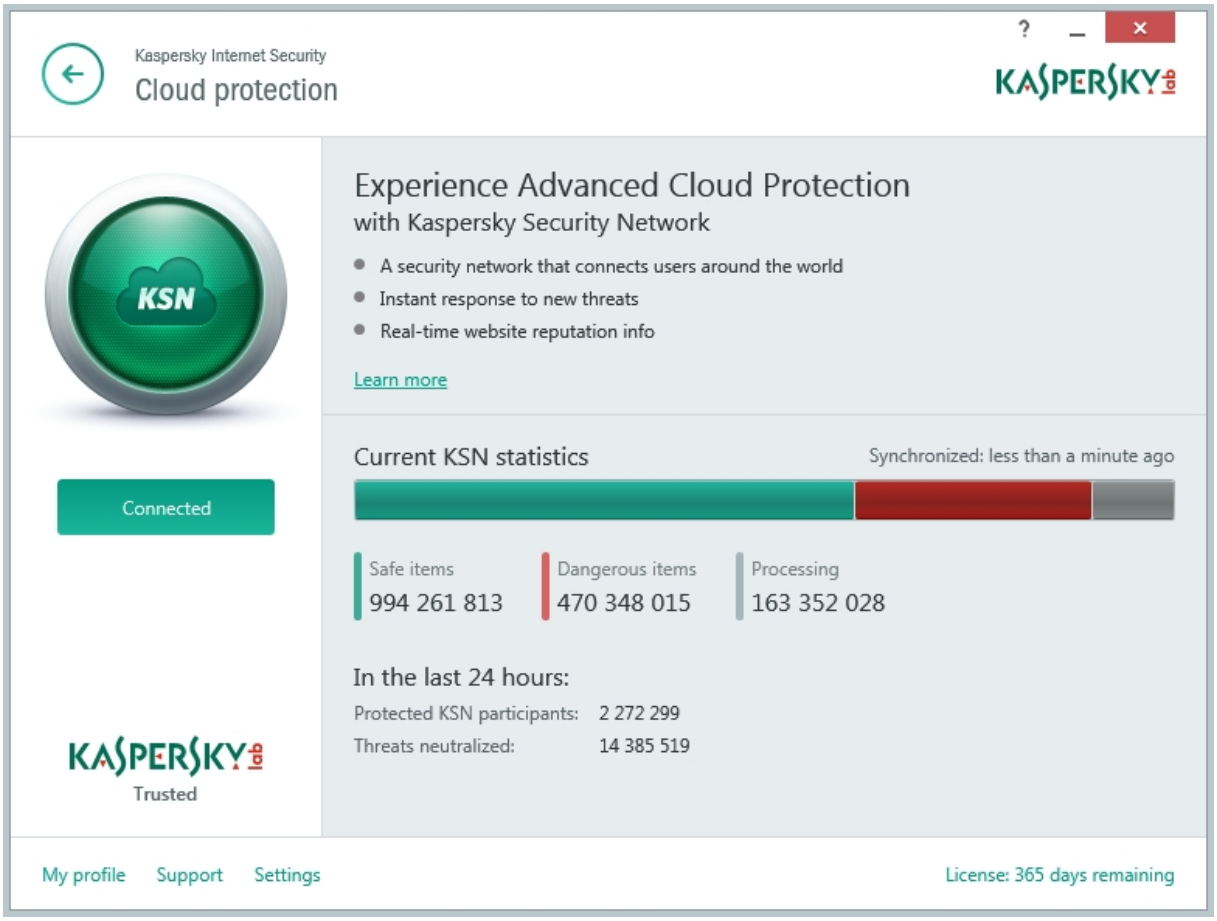
1. Statistics regarding detected threats and suspicious activities are sent to Kaspersky Lab's cloud infrastructure. If the Kaspersky Lab databases contain no corresponding records for a given sequence of indicators (for example, if the detection was made by means of heuristics), the data progresses to an automated analysis system that is able to recognize most new cyberthreats. This system draws on Kaspersky Lab's powerful resources instead of having to rely on those of the user's devices. In cases where it cannot automatically render a verdict, Kaspersky Lab's experts manually analyze the information.

2. If the code or URL turns out to be malicious, the details are added to the Urgent Detection System database and made available to all users within minutes of the initial detection. At the same time, records for legitimate applications are added to the Whitelisting database.
3. After further analysis of a suspicious code or URL, the system or Kaspersky Lab's analysts determine how dangerous it is and add the description to a signature database that is regularly downloaded onto every computer protected by Kaspersky Lab's solutions.
4. If Kaspersky Lab users encounter an already-known cyberthreat (which is not yet in signature databases), the solution sends a request to KSN and receives an immediate verdict, thereby ensuring the highest level of protection.



Kaspersky Security Network for consumers

Apart from the general benefits of cloud-assisted protection, Kaspersky Lab's consumer products allow users to receive statistics from the Kaspersky Security Network, including figures for the number of users protected, malicious objects blocked and legitimate data processed:

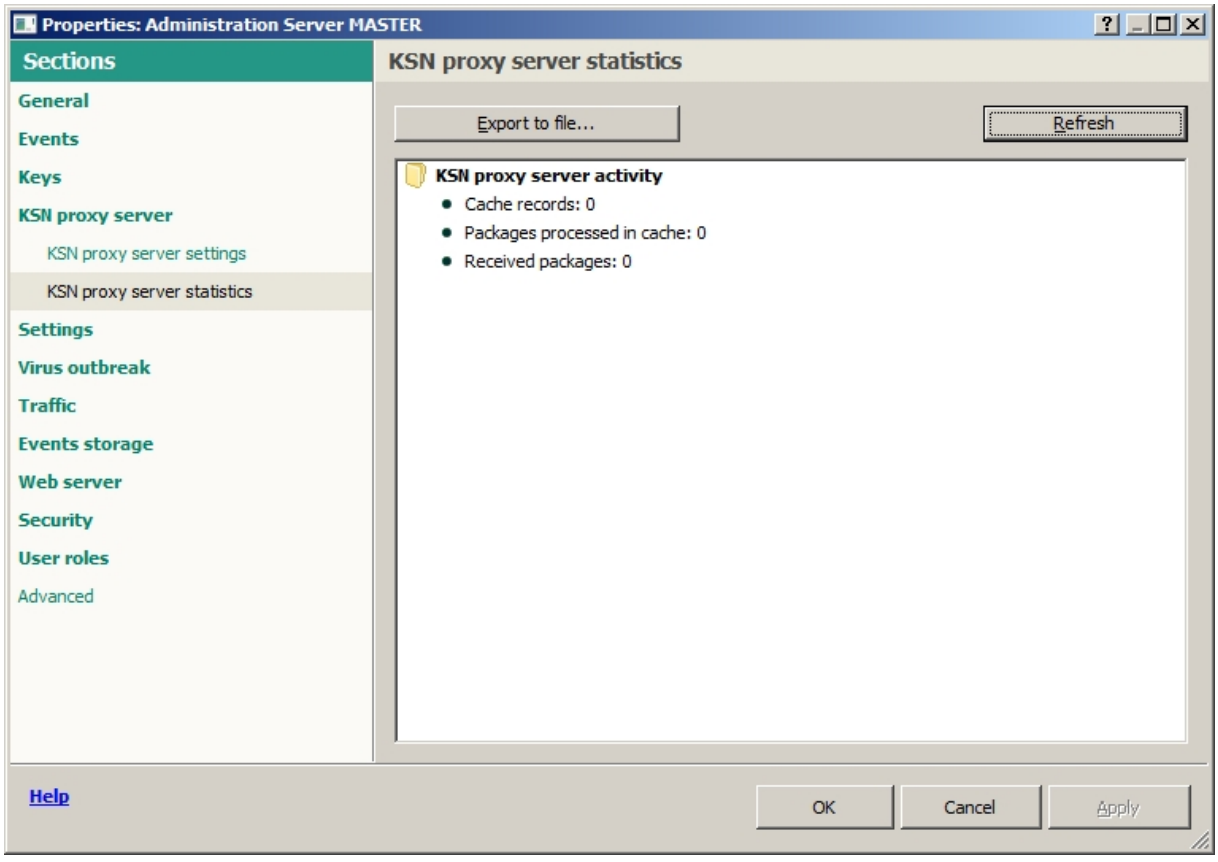


Another feature available in Kaspersky Lab's consumer products is the ability to check the reputation of any executable file based on data from the Kaspersky Security Network. Such queries return a verdict on the file in question (whether the program is legitimate or not) as well as the date when the file first appeared, its popularity by country and other data (the reputational technology is called 'Kaspersky File Advisor'). This feature allows users to do a basic check of unknown programs before launching them, although the same information is obtained automatically when a user tries to execute a file.

Kaspersky Security Network for businesses

There are a number of functions in the Kaspersky Security Network specifically for corporate products. First, the cloud-assisted protection technology is used for application whitelisting, using data from the Kaspersky Security Network. Known legitimate files are automatically grouped into categories, such as games, commercial software, etc. Using these categories, a systems administrator can quickly establish and apply certain rules for specific types of software, in line with their security policy. The data for the Application Whitelisting database is supplied by more than 400 leading software vendors and is used along with “crowd-sourced” information.

The Kaspersky Security Center management solution provides businesses with granular controls over how the Kaspersky Security Network protects corporate endpoints. The administrator can select whether cloud-based protection is enabled or disabled in the specific modules of Kaspersky Endpoint Security for Business. It is also possible to disable the sending of data to the Kaspersky Security Network. In order to reduce bandwidth usage, an internal Kaspersky Security Network proxy may be installed inside the local network to cache data from KSN. IT departments can always monitor traffic sent to KSN if needed:



The benefits of Kaspersky Security Network

Today, Kaspersky Security Network technology is used on millions of computers around the world, providing a detailed global picture of how new cyberthreats evolve and circulate, where they originate and how many infection attempts occur within given periods of time. The globally-distributed cyberthreat monitoring carried out by the Kaspersky Security Network makes it easy to respond quickly to new threats no matter where the sources and targets are located.

The Kaspersky Security Network helps to build an efficient, proactive defense. It helps to identify and block new threats before they become widespread and can cause any significant damage to the client's IT network. Such a proactive defense system is essential to ensure the stable and uninterrupted operation of IT equipment and the business processes it supports.

[i] *Depends on the product (see the corresponding license agreements).*