KASPERSKY lab

Kaspersky Security Network

The Kaspersky Security Network (KSN) is a complex distributed infrastructure dedicated to intelligently processing cybersecurity-related data streams from millions of voluntary participants around the world. By analyzing these data streams automatically in the cloud, the system ensures the fastest reaction times to new and yet unknown cyberthreats and the maintenance of the highest levels of protection for every partner or customer.

KSN also employs Kaspersky Lab's HuMachine principle: both our expert knowledge and our next-generation machine learning capabilities are merged, allowing us to spot patterns, changes and new threats in the cyber landscape with accuracy and skill.

Protection from unknown and advanced cyberthreats

Today, the Internet is an integral part of people's lives, but it is also the source of growing risks. In Q1 2017 alone, Kaspersky Lab products detected 479 million malicious attacks and 51 million attempts to open a phishing site on users' devices, nearly a twofold increase compared to Q1 2016. However, cybercrime has grown not only in volume, but also in sophistication. Kaspersky Lab's stats show that just 70% of the threats faced by users every day are known, while 30% are unknown and advanced ones demanding additional layers of protection. The growing number and complexity of threats requires a specific approach to cybersecurity. That is why traditional on-premise 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 continuously updated information about new threats. The four main benefits of using cloud protection are:

- Better detection rates
- Reduced reaction time to new threats
- Minimization of false positives
- A 'lighter' product for the user

The basic principles of the Kaspersky Security Network

- Information processed is limited to that needed in order to improve detection algorithms, refine the products' operation and offer better solutions to our customers;
- The information processed is received from customers who have accepted an End-User License Agreement (EULA) and KSN agreement where the kind of information obtained is described in full[1];
- Participation in the KSN agreement can be opted in or out of, at any time, in the solution settings;

- The data received by KSN is not attributed to a specific individual. The information is used in the form of aggregated statistics, on separated servers with strict policies regarding access rights;
- The information shared is protected, even during transit in accordance with legal requirements and stringent industry standards, including through encryption, digital certificates, firewalls and more.

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' devices, analysis of the data received in order to determine new threats, and the delivery of relevant intelligence and countermeasures to protected customers. The information about infection attempts is analyzed using the company's powerful in-house expertise and technological resources – both automated and human.

The safety of a program is determined through multi-layered checks with the help of machine learning, including checking the behavior's reputation in the cloud – if it's known as dangerous, checking the source and integrity of the program, and many other factors.

A website's safety is determined through checking the company's digital certificate and verifying this certificate's legitimacy, the analysis of webpage content for potential threats and traps, and its URL for its reputation in the cloud, and many other factors.

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.

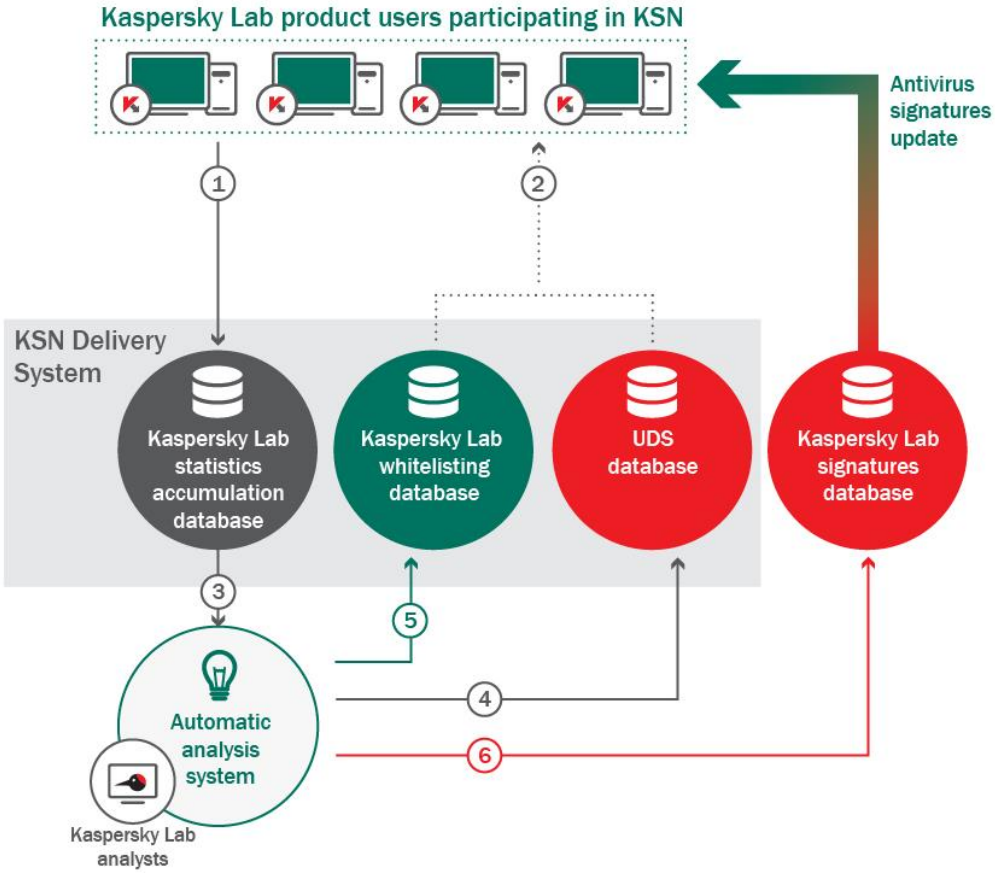
If it is not possible to determine the level of threat posed by an object, the data is sent to Kaspersky Lab experts, who conduct additional in-depth analysis before adding the data to KSN for instant detection through the cloud. This step is crucial as it allows KSN, like every other Kaspersky Lab solution, to fuse next generation machine power with human expertise.

While creating and uploading the entry to a traditional antivirus database takes hours, KSN users receive a corresponding measure of protection within minutes of the launch of a cyberattack. KSN therefore assists both database 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 five different phases:

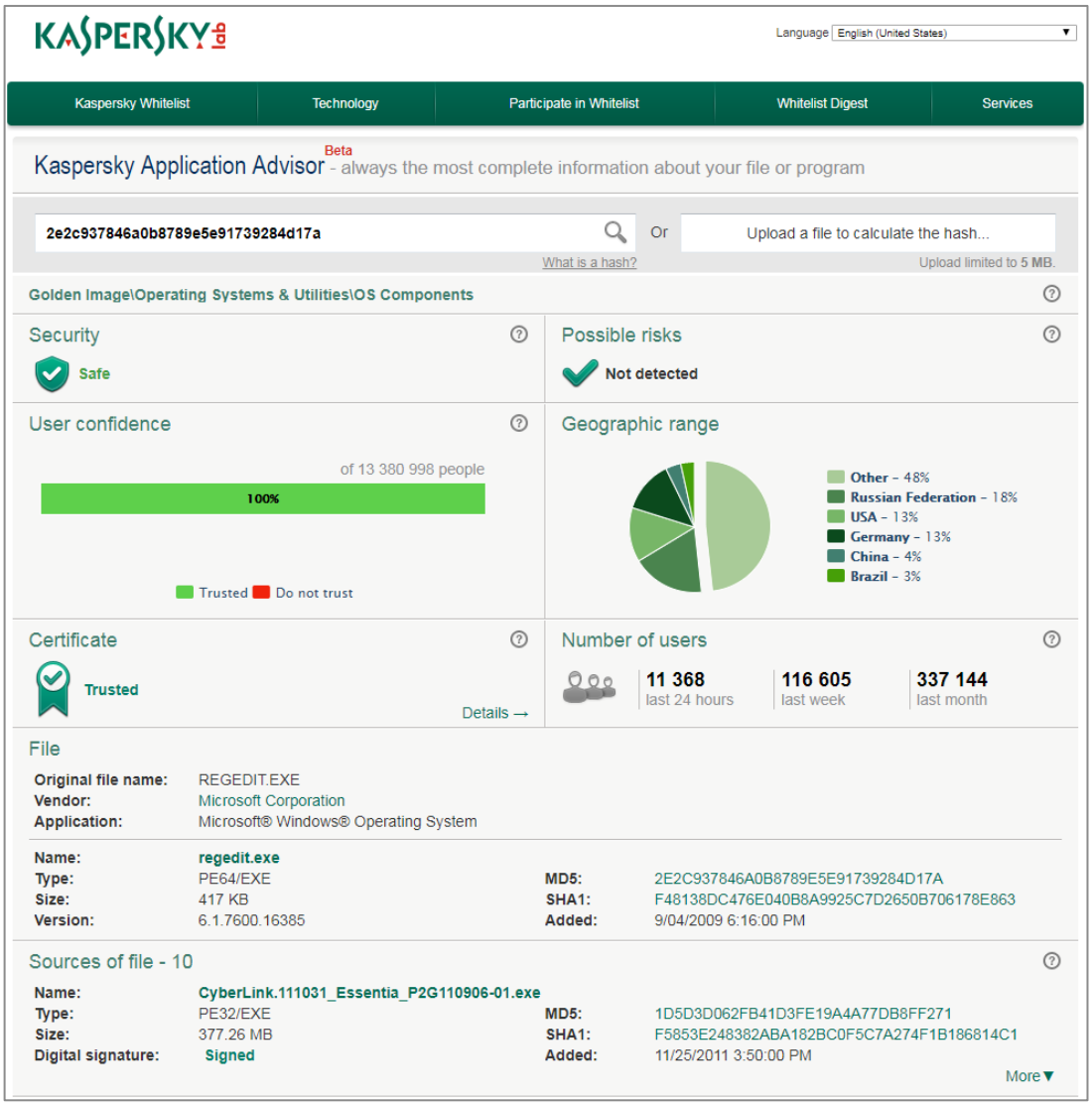
1. The product on the device detects suspicious activity which is not determined as malicious by default on-premise and sends this information to Kaspersky Lab's cloud infrastructure.
2. If Kaspersky Lab users encounter an already-known cyberthreat (which is not yet in the threat databases), the solution sends a request to KSN and receives an immediate verdict, thereby ensuring the highest level of protection.
3. If the Kaspersky Lab databases contain no corresponding records for a given sequence of indicators, the data progresses to an automated analysis system that is able to recognize most new cyberthreats. This system draws on Kaspersky Lab's powerful human and machine resources instead of having to rely on those of user devices – with Kaspersky Lab's experts manually analyzing the information when big data analysis cannot automatically render a verdict.
4. 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 (and when the solution sends a request to KSN, it receives an immediate verdict on this threat).
5. If the code or URL turns out to be legitimate, their records are added to the whitelisting database.



Kaspersky Security Network's front-end servers are located in different countries around the world (Germany, Canada, China etc.), while the back-end servers are located in Russia, where the largest part of Kaspersky Lab's anti-malware research team works.

Kaspersky Security Network for consumers

Apart from the general benefits of cloud-assisted protection, Kaspersky Lab's consumer products allow users to check the reputation of any file or program on the device based on data from the Kaspersky Security Network. The reputational technology is called 'Kaspersky Application Advisor':

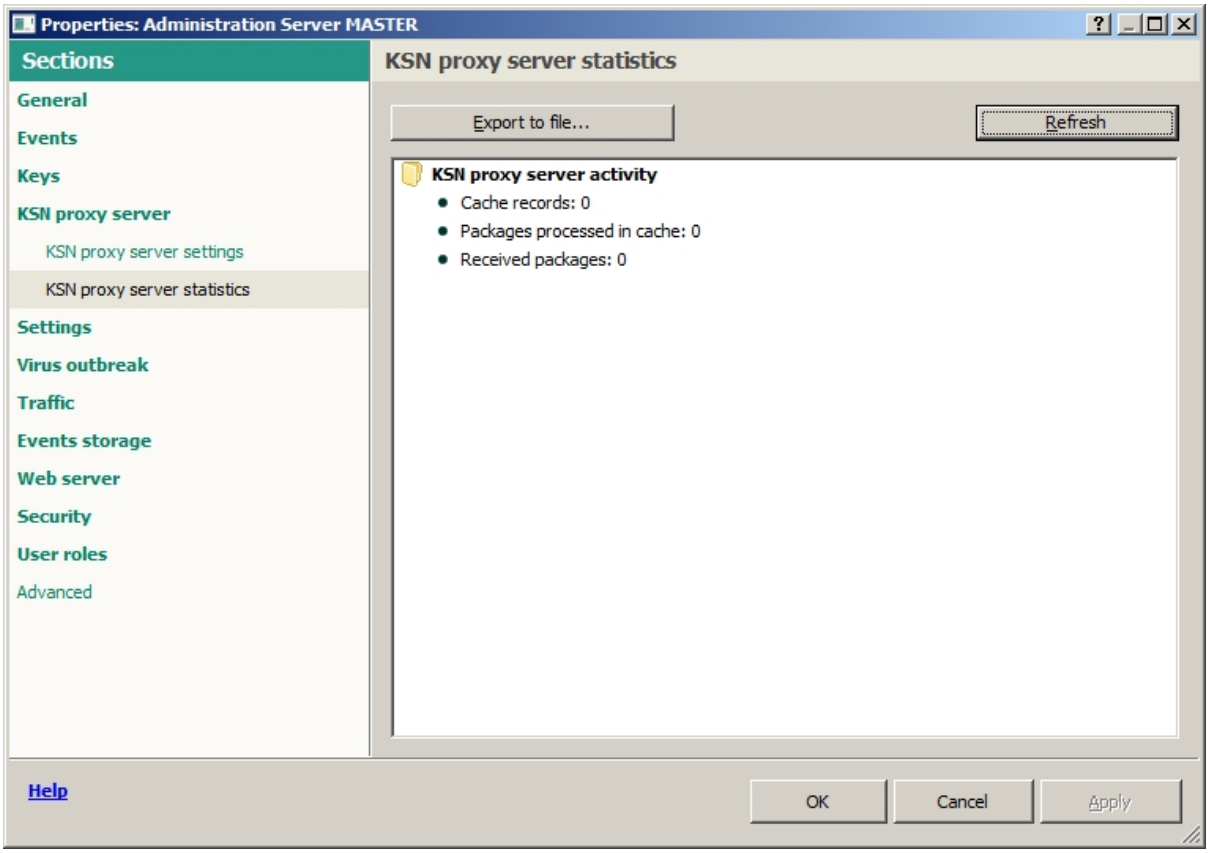


Such queries return a verdict on the file in question (whether the program is legitimate or not) as well as the date when the file first appeared, its popularity by country and other data. This feature allows users to do a basic check of unknown programs before launching them, although the same information 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 600 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. Its accuracy is ensured by the well-oiled mechanism of interaction between robots and experts – Kaspersky Lab's HuMachine approach. With this powerful combination, KSN helps to identify and block new threats before they become widespread and can cause any significant damage to the client's IT network.

This proactive defense system is essential to ensure the stable and uninterrupted operation of IT equipment and the business processes it supports - it is crucial for businesses and consumers that wish to benefit from next generation cybersecurity.

[1] The content depends on the product and can be found in the "Support" sections of local Kaspersky Lab web-sites