



# Cloud-based technology in Kaspersky Security Network

Kaspersky Security Network is a progressive technology implemented in the latest versions of Kaspersky Lab's consumer and business products. When it comes to new malware, it ensures a prompt response and an unprecedented level of detection that provides outstanding protection. Kaspersky Security Network not only allows previously unknown threats to be detected and blocked but can also locate and blacklist the online source, protecting users from subsequent threats that emerge from the same sources.

For corporate users Kaspersky Security Network offers additional benefits, in terms of enhanced control of applications and whitelisting for known legitimate applications. Kaspersky Security Network combines the capabilities of continuous globally distributed monitoring of real-life threats, a centralized analysis of threats using Kaspersky Lab's substantial expert and technology resources, and the immediate generation and distribution of protection measures. This produces a powerful synergy effect, providing users of Kaspersky Lab products with comprehensive real-time protection against new malware.

## Quick, timely protection from cyberattacks

Malware such as viruses, worms and Trojans, have become the principle threat to the normal functioning of computers and to the information stored in them. The scope and range of malicious software is constantly expanding, presenting an ever-growing security challenge. According to Kaspersky Lab internal data, about 200,000 new samples of malware appear "in the wild" every day. Malicious programs are also making use of new methods to penetrate computer systems, concealing their activities and bypassing detection by security software. No conventional malware detection method can now provide complete protection when used as a stand-alone tool.

Today's computer world requires a new, integrated approach to ensure computer security. This approach needs to combine the advantages and minimize the deficiencies of the traditional methods of combating malicious software, as well as harnessing the potential of global monitoring and automatic updating of new real-life threats. This is the approach implemented in Kaspersky Security Network.

## The basic principles of Kaspersky Security Network

Kaspersky Security Network includes several subsystems: continuous geographically distributed global monitoring of real-life threats on users' computers, instantaneous delivery of collected data to Kaspersky Lab's host servers, analysis of that data and the creation of protection measures against new threats, and the fast distribution of those measures to users.

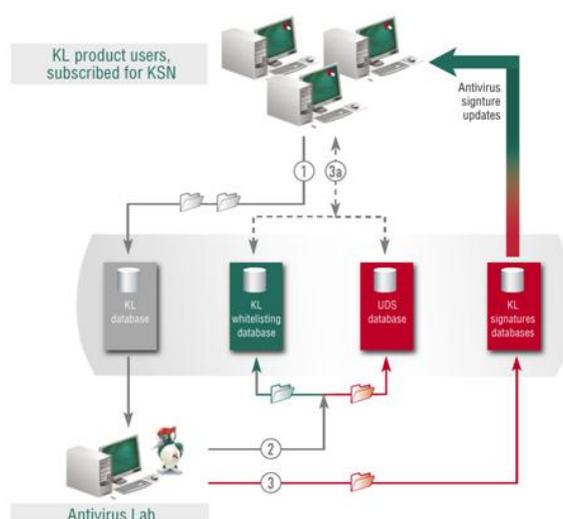
Kaspersky Security Network automatically collects information about attempted infections and sends the data to Kaspersky Lab. Information about suspicious files downloaded to and executed on users' computers is also collected, regardless of their source (websites, email attachments, peer-to-peer networks, etc.). This is done strictly voluntarily and confidentially – a user of one of Kaspersky Lab's consumer products has to agree to participate in the system. Users of Kaspersky Lab's corporate solutions do not participate in the formation of the Kaspersky Security Network database. In any case, no personal information such as passport data, passwords or any other personal details is collected.

The information collected on attempted infections is sent to Kaspersky Lab's central servers and analyzed using the company's powerful in-house technology and expert resources. This ensures extremely fast and reliable detection of

new software, whether malicious or secure. The decision on the safety of a program is made based on the availability of a digital signature verifying the source and integrity of the program, as well as a number of other factors. A program recognized as secure is entered to the list of trustworthy applications.

A program is deemed malicious after the required detection procedures are complete. As soon as a program is deemed malicious, it is reported to Kaspersky Lab's Urgent Detection System, so that the information becomes available to Kaspersky Lab product users even before the signature for that piece of malware is created and updated on their computers. In that way Kaspersky Lab's clients receive prompt information about new and unknown threats minutes after the launch of a cyberattack, compared to hours for traditional signature database updates.

If a program is launched by a user, it is checked against whitelists and Urgent Detection System lists, and is granted rights to access computer resources or blocked accordingly. Kaspersky Security Network technology plays an important role in replenishing these lists and keeping them up to date, ensuring reliable control over applications.



*Kaspersky Security Network flowchart*

This flowchart describes the basic principles of how users of Kaspersky Lab's products interact with KSN. This interaction includes 4 different phases:

1. Information on the newly launched or downloaded applications and visited web pages (URLs) is sent by users of the relevant Kaspersky Lab consumer and corporate products.
2. The files and URLs are checked and added to the Urgent Detection System database if they turn out to be malicious. Legitimate files are added to the "Whitelisting" database.
3. Kaspersky Lab's experts finish the analysis of suspicious files, determine their degree of risk and add the description to signature database.
- 3a. Information about newly discovered malicious and legitimate files and URLs becomes available to all users of relevant Kaspersky Lab products (not only the subscribers of Kaspersky Security Network) minutes after the initial detection.

After the analysis of a new malicious program is completed, a signature is also generated and placed in the antivirus databases that are regularly updated on computers of all Kaspersky Lab users.

Whitelisting is not the only technology that allows users to make a decision about a program with the assistance of KSN resources. The system includes the reputational technology 'Wisdom of the Crowd' (WoC), which provides information about how popular a certain program is and its reputation among other users – the members of KSN.

---

Moreover, the latest versions of Kaspersky Lab products include an opportunity to get Global Security Ratings (GSR) direct from the cloud. Each GSR is calculated using a flexible, customizable algorithm and various reputational data.

Kaspersky Security Network therefore makes use of a combination of signature and heuristic malware detection methods as well as application control technologies using white- and blacklists, WoC and GSR.

## Enhanced cloud security for businesses

The benefits of Kaspersky Security Network are also available to Kaspersky Lab's corporate customers. Along with traditional protection techniques and advanced tools to enforce corporate IT security policies, Kaspersky Security Network brings a prompt reaction to new and unknown threats and helps to secure confidential data against targeted attacks.

The general principles of using Kaspersky Security Network in the business environment are the same as those for Kaspersky Lab's consumer products. The company's Windows-based endpoints use data from Kaspersky Security Network to evaluate the reputation of files and website URLs, and, based on that, block access to malicious content or apply certain restrictions on suspicious software. At the same time Kaspersky Security Network provides immediate, real-time protection against new and emerging malware threats to corporate smartphones and tablets.

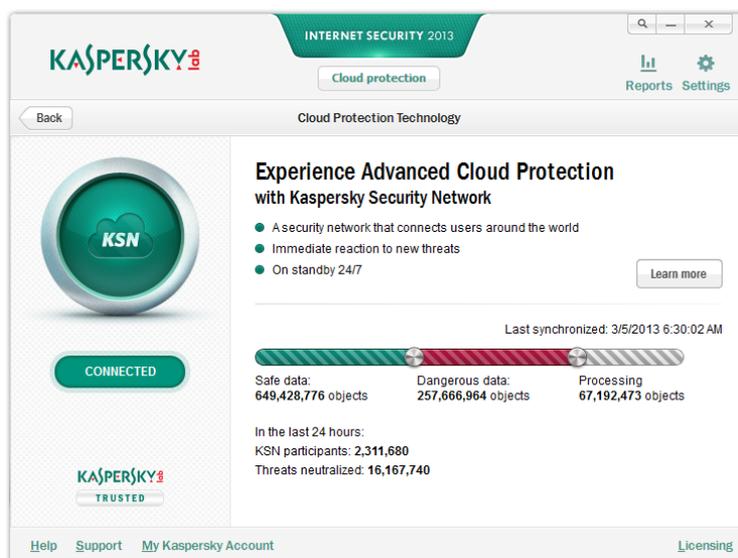
There are a number of enhancements in Kaspersky Security Network functionality for corporate products including a new platform - Kaspersky Endpoint Security for Business. First, cloud-assisted protection technology is used for application whitelisting, utilizing data from Kaspersky Security Network. Known legitimate files are automatically grouped in categories, such as games, commercial software, etc. Using these categories a systems administrator can quickly set up and apply certain rules for specific types of software, according to security policy. Further data for Application Whitelisting is supplied by more than 200 leading software vendors and this is used alongside the "crowd-sourced" information. Some targeted security solutions also use Kaspersky Security Network functionality. For example, Kaspersky Security for Mail Server uses cloud-assisted technology to track new malicious objects and unwanted messages in email traffic.

Kaspersky Security Center provides businesses with granular controls over how Kaspersky Security Network is used to protect corporate endpoints and servers. The administrator can select whether cloud-based protection is enabled or disabled in each specific module of the Kaspersky Endpoint Security for Business platform. To comply with certain security policies, it is also possible to disable the transmission of data to Kaspersky Security Network. In order to reduce bandwidth usage, an internal Kaspersky Security Network proxy can be installed inside the local network.

## Cloud-based protection for consumers

The latest versions of Kaspersky Lab consumer products, namely Kaspersky Internet Security 2013 and Kaspersky Anti-Virus 2013, enjoy full support from the cloud-based Kaspersky Security Network. Apart from the general benefits of cloud-assisted protection, the consumer products allow users to receive general statistics about Kaspersky Security Network: the number of users protected, malicious objects blocked and legitimate data processed.





Another useful feature is the ability to check any executable file for its reputation based on data from Kaspersky Security Network. A query returns a verdict on the file in question (whether the program is legitimate or not) as well as information about 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.

One of the distinctive features of Kaspersky Internet Security 2013 is its cloud-assisted anti-spam technology. It uses information from Kaspersky Security Network to detect and block unsolicited messages, and does not require any training of the anti-spam filter, as in previous versions of this consumer product. The cloud-based anti-spam feature is region- and language-dependent and may not be available in some countries.

## The benefits of Kaspersky Security Network

Uninterrupted global monitoring of new threats and threat sources, as well as the immediate availability of new protection measures ensure an unprecedentedly rapid response to new threats and an unrivalled protection service for Kaspersky Lab's clients.

Today, Kaspersky Security Network technology is used on millions of computers around the world, presenting a detailed global picture of how new malware evolves and circulates, where new threats originate and how many infection attempts occur within specific time periods. Kaspersky Security Network's globally distributed malware monitoring provides an effective response to new threats no matter where the sources and targets are located.

Real-time malware monitoring on user machines helps track actual threats and block them in their "in-the-wild" environments as soon as an infection attempt takes place.

Continuous malware monitoring and immediate reporting of suspect files to Kaspersky Lab ensure that malware databases and protection measures to combat these threats are always up to date. Automation ensures a much faster, more accurate and complete response than conventional manual reporting of suspicious files to the antivirus vendor via email.

Strict confidentiality is guaranteed: personal information such as usernames, passwords, personal data and the contents of documents is not collected or transferred to Kaspersky Lab servers.

The latest Kaspersky Lab products also utilize Kaspersky Security Network to block links leading to fraudulent and malicious websites more effectively. Web links are first checked against a local database of phishing and malicious websites and if no match exists, they are further checked against KSN's online blacklists. If they are unknown, they are heuristically analyzed for the presence of attributes associated with malicious links. Detecting dangerous links

---

has become more accurate because KSN's online databases have accumulated a large amount of additional information about various websites since the 2011 product versions of consumer products were released.

Overall, users of Kaspersky Lab products which are supported by Kaspersky Security Network enjoy more complete protection against personal data theft, as new malware designed to steal personal or business data is blocked on their computers. That means no programs spying for files stored on the hard disk, keyloggers, screenshot senders, network activity spies, etc.

Kaspersky Security Network provides proactive defense, i.e., it identifies and blocks new threats before they become widespread and can cause any significant damage to users' machines. A proactive defense system is essential to ensure the stable and uninterrupted operation of IT equipment and the business processes it supports.

