Kaspersky® Private Security Network

Kaspersky Security Network: Big Data-powered Security

Protection against every next generation of threats

The number of cyberattacks globally increases every day. This has a significant impact on business, often resulting in data theft or loss of important information, which threatens business processes of all company types and sizes, from start-ups to industry leaders.

But it's not just about the number of attacks: new generations of malware appear every day, many of them are using new, sophisticated tricks designed to bypass existing security solutions. In this constantly shifting environment, protection is only as effective as a vendor's ability to closely monitor the threat landscape and distill data into actionable Security Intelligence and new technologies.

In this never-ending arms race, a true cybersecurity solution is capable of instant, effective response to new malware while striving to anticipate cybercriminals' next moves. A key component of that capability is the use of cloud technologies that apply distributed data mining and Data Science technologies to threat information processing. The most capable of these systems, like Kaspersky Security Network, have globally distributed data acquisition points and powerful Big Data processing facilities to significantly speed up transformation of raw data into actual protection. Human expertise is a vital part of this data processing cycle, ensuring a proven high detection rate – and the Best Possible Outcome for customers.

Three key components are needed for the successful operation of this mechanism:

- Acquisition of global malware detection statistics along with real-time data on suspicious activities
- Big Data processing and analysis
- Fast delivery of Security Intelligence to customers

The hardest stage of this is sorting and analyzing data. Volumes are so large they require the use of Data Science–based automation capable of digesting the incoming Big Data. Human expertise nonetheless remains an important advantage of this system, because only human intuition and experience can help machines to cope with the complex and often highly imaginative creations of malware authors. Kaspersky Lab's experts have real-time access to all the information being gathered, enabling them to gain valuable new insights into threats, apply knowledge to investigations and develop new, proactive detection technologies. The most significant of the many customer benefits of our approach include:

- Best detection of advanced and previously unknown malware
- Reduced detection errors (false positives)
- Significant reduction of response time to new threats – traditional signature-based responses can take hours, KSN takes about 40 seconds.

KSN basic statements

Using real-time data from millions of volunteer endpoint sensors globally, every file that passes through Kaspersky Lab protected systems is subject to analysis based on the most relevant threat intelligence. The same data ensures the most appropriate action is taken. Participation in KSN is completely voluntary and all acquired statistics are anonymized, with absolutely no connection of data to specific users; full details of the types of data collected and how it's transferred are available in the EULA.

KSN uses a fully secured connection to send information. The data transmission system is built to industry standards. All primary data processing is done automatically, and access is only available in exceptional, serious cases.

Fig.1 – Scheme of data transmission between KSN elements

Astraea – smart system with Big Data analytics

Hundreds millions of different records come to KSN every day, a massive volume of data often reaching hundreds of gigabytes daily. This anonymized data is compressed and stored for future use; even after compression, it still requires terabytes of storage.

One of the systems Kaspersky Security Network uses to process this enormous data stream is called Astraea. Every day, it processes information on millions of objects, sorting and analyzing it. Once sorted, Astraea rates each object; only the metadata of the object used for the analysis, but not its contents.

Every suspicious event received by the system is evaluated by its importance and potential danger using multiple different criteria. Following this analysis, the object's reputation is calculated, and global statistics about it are requested. What else can the collective intelligence tell us about it? Perhaps its reputation is even worse than it initially seems? Or is it a false alarm? This querying against other information allows the system to fine-tune verdicts and reduce the probability of false positives for other users.

When an object's accumulated statistics confirm that it's malicious, secure or unknown status, that information is made available across all supported Kaspersky Lab products where users have enabled Kaspersky Security Network – without any human intervention.

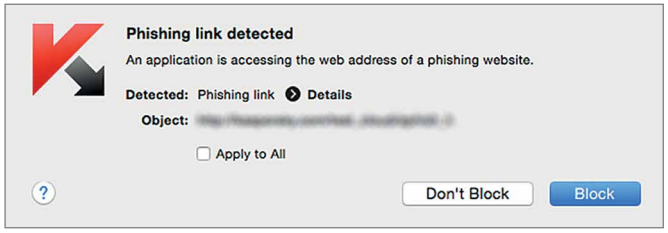

Fig. 2 – Dangerous site alert

Similarly, when malicious web resources are processed, users automatically receive a warning of the danger when they try to access it.

For all the advantages of automation, protection without people is impossible, because system has to withstand living cybercriminals' tricks and evasion techniques. That is why the KSN, like in other systems of Kaspersky Lab, employs the HuMachine principle: the fusion of machine power and the human experience of experts. How does it work?

If you can't determine the level of threat posed by an object, the data is sent to experts, who conduct additional in-depth analysis before adding the data to KSN for instant detection through the cloud. At the same time, heuristic detection models can be adjusted to detect many different malware specimens based on the similarity of indicators.

Astraea is a highly intelligent system that constantly learns to effectively cope with the rapidly changing landscape of threats. However, the old learning criteria are gradually becoming irrelevant, and it is necessary to identify and introduce new ones to effectively counter the new "inventions" of the attacking side. To do this, machine also needs the help of experts.

From experts – to real life

Security Intelligence delivery from KSN is fast – it's measured in seconds. This maintains a consistently high level of protection against real-world, real-time cyber threats. In the event of a mass attack, when the information about the malware has already reached KSN servers, but has not yet been delivered to end-users in the form of detection records, the system will provide it immediately in response to a request from the user.

Of course, this requires some bandwidth, and Internet traffic may be limited. Therefore, KSN can use local

caching servers installed within the local network, which helps to reduce the load on the Internet connection.

If the user has switched off KSN, they'll only receive accurate information about new malware following an update; before this, they'd continue to be protected by other proactive mechanisms.

KPSN

While all information processed by Kaspersky Security Network is completely anonymized and disassociated from its source, Kaspersky Lab recognizes that some organizations – for compliance or company policy reasons - require absolute lock-down of data. This has traditionally meant that enterprises can't avail of cloud-based security services.

For these customers, Kaspersky Lab has developed a standalone product: **Kaspersky Private Security Network**, allowing enterprises to take advantage of most of the benefits of global cloud-based threat intelligence without releasing any data whatsoever outside their controlled perimeter. It's a company's personal, local and completely private version of Kaspersky Security Network.

KPSN can be installed on a special, local server, providing adaptive protection to all connected devices. KPSN does not mandate access to Internet: in particularly strict use environments, updates can be done manually using secure portable media. In any case, the provision of an inbound data stream greatly boosts reaction times to constantly shifting threats:

Conclusion

The need for immediate protection against new threats is obvious, even to people who are not directly involved into information security. Even without Kaspersky Security Network enabled, the multiple layers of protection technologies in our solutions provide effective security for all users.

What KSN's instant, cloud-based protection also adds to the mix is support for additional, important security mechanisms that minimize false positives while increasing detection quality through the use of real-time, additional data on threats, authorized applications and other relevant information.

Given that the more complex and focused threats tend to inflict damage that's incomparably greater than in case of the mass malware, the value of the Security Intelligence delivered by means of Kaspersky Security Network cannot be overestimated. The highest accuracy of the information is ensured by the well-oiled mechanism of interaction between robots and experts: Kaspersky HuMachine. For any business it is essential to ensure the Best Possible Outcome in any situation, and Kaspersky Security Network, as well as its "private" version, effectively serves achieve this goal.

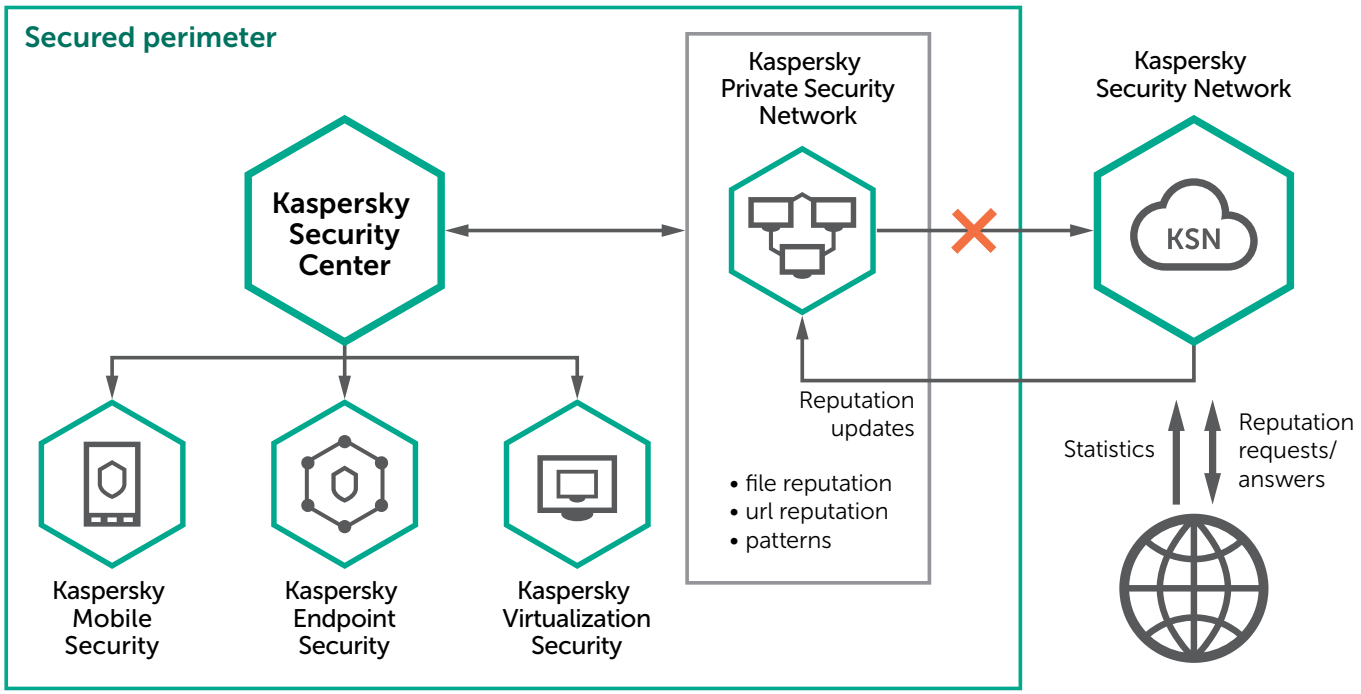

Fig.3 – Scheme of KPSN infrastructure in secured perimeter

All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com
#truecybersecurity