KASPERSKY lab

KASPERSKY PRIVATE SECURITY NETWORK: REAL-TIME THREAT INTELLIGENCE – INSIDE THE CORPORATE INFRASTRUCTURE

Global threat intelligence
for local implementation

www.kaspersky.com

A CLOUD-BASED THREAT LABORATORY FOR KASPERSKY LAB CUSTOMERS

Since 2008, Kaspersky Lab's cloud-based threat intelligence (Kaspersky Security Network) has provided real-time reputation data and threat information to millions of customers around the world. Using anonymized data from 80 million volunteer endpoint sensors globally, every file that passes through Kaspersky Lab-protected systems is analyzed using the most relevant threat intelligence.

It takes up to four hours for standard security solutions to receive the information needed to detect and block up to 360,000 new malicious programs discovered by Kaspersky Lab researchers every day. Threat intelligence sharing via Kaspersky Private Security Network provides this information in 30-40 seconds – from within the organization.

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. That's it: it's a company's personal, local and completely private version of Kaspersky Security Network.

To understand how Kaspersky Private Security Network works, let's start by taking a look at Kaspersky Security Network.

Kaspersky Security Network is available as an optional, complementary component of Kaspersky Enterprise Security for Business, Kaspersky Security for Virtualization, Kaspersky Security for Storage, Kaspersky Security for Data Centers, Kaspersky Anti-APT and Kaspersky Fraud Prevention solutions.

REAL-TIME THREAT INTELLIGENCE, DELIVERED BY THE CLOUD

Kaspersky Security Network (KSN) uses the high performance capabilities of the cloud to ensure the fastest threat detection and response times. On-the-fly information on the latest threats is sent to our secure cloud for analysis; every time a Kaspersky Lab-protected system detects a suspicious file, application or web site, it can be queried against the cloud-based threat information and a verdict on its security status delivered immediately. Conventional techniques typically take hours to update databases with new threat information, while on-system or local threat analysis is a drain on resources.

Contributing to a higher level of security

Each participating KSN node delivers unique insight into the threats our users face, contributing to a body of threat intelligence that makes the Internet safer for everyone. A good example of just how powerful that insight can be: KSN detected modules of the highly sophisticated Equation targeted attack – long before it was identified as a concerted, organized threat group. Equation's Trojan dropper, "EquationLaser" and the worm "Funny" were detected and blocked by KSN in April 2012 and June 2013, respectively.

What makes KSN's role in detecting the Equation APT so interesting is that it illustrates perfectly the role that home and small business participants can play in contributing to sophisticated threat research. Many of these users participate in KSN and we learn a lot from the threat information they contribute; surprising as it may seem, home and small business users are an extremely valuable source of threat intelligence for enterprise customers. This is partly because they tend to engage in higher-risk behaviours online but also because cybercriminals often use them as a springboard to launch attacks on more secure enterprise networks.

Let's take a look at how KSN's cloud-based protection uses this data to provide better detection rates, reduce reaction times, minimize false positives and support whitelisting.

DETECTION RATES MATTER

Kaspersky Lab analysts detect 360,000 new malicious files every day; 113,500 phishing 'wild cards' are added to our anti-phishing database each month.

Cybercrime has grown, not only in volume, but in sophistication; while 70% of the threats faced by enterprises every day are known ones, 30% are unknown, advanced ones that traditional, signature-based security on its own can no longer address. Threat intelligence garnered from 24-7 expert monitoring of the kinds of attacks our users experience and rebuff forms a key component of Kaspersky Lab's multi-layered defense system. And Kaspersky Security Network (KSN) plays a key role in delivering that insight.

KSN processes more than 600,000 requests, carrying 14Gb of incoming global statistics per second – this constantly updated intelligence enables increased detection rates of 2.5 – 3.1% for KSN users. In the past year, over 39% of KL users faced threats so new and unknown that standard anti-virus components were unable to detect them; KSN successfully detected these. A full 20% of the threats detected by Kaspersky Lab technologies are detected using the statistics gathered by KSN.

Think about it: in the current threat environment, even a 0.9% difference in detection rates can translate into hundreds of thousands of pieces of malware slipping through the net over the course of a year. And it's that 1% of targeted attacks that are usually the most harmful to enterprise systems, often going undetected for months or even years.

That extra sliver of expertise and protection provided by KSN could represent the very threats your organization most needs to avoid – especially when it comes to APTs and more advanced malware. 'Kill chain' analysis shows that attackers must progress successfully through each stage of the chain in order to achieve their objective; just one mitigation disrupts both the chain and the attacker.[1]

[1] EM Hutchins, MJ Cloppert, RM Amin: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

TIMING IS EVERYTHING

If reducing the number of threats slipping through the net is important, so is the amount of time it takes to detect and respond. KSN's cloud-based detect-and-block speeds are significantly higher than those offered by traditional anti-malware updates. Standard signature update and release processes can take hours and there's little scope for improving on that. Cloud-assisted updates like KSN's, on the other hand, enable near real-time threat intelligence sharing on new and emerging threats, suspicious behavior patterns, malicious links or dangerous web sites – all within 30-40 seconds.

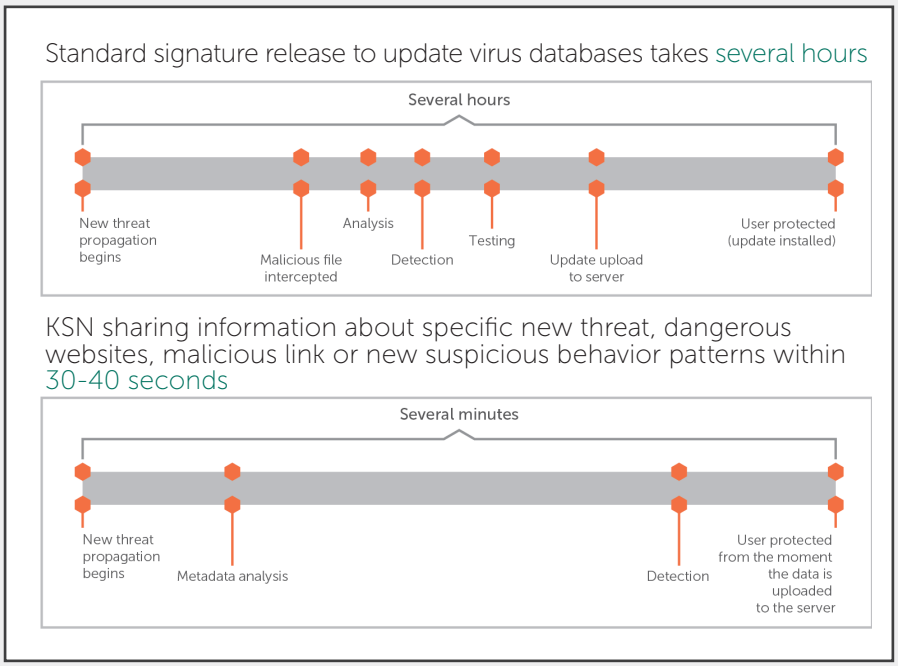


Figure 1: Reducing threat reaction times with Kaspersky Security Network: real time, proactive, global view.

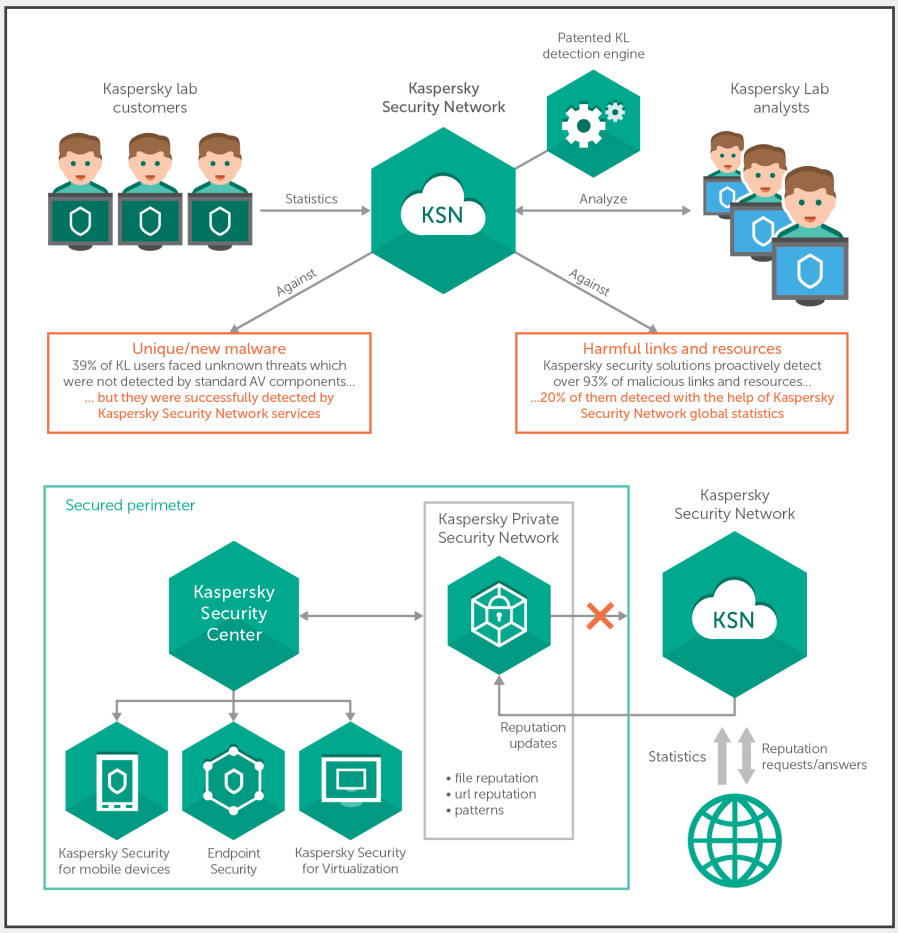
Think about it: when it comes to sophisticated, advanced threats, a delay in response of even a few hours can lead to serious consequences.

ELIMINATING FALSE POSITIVES

In any system that scans large volumes of files, false positives can become an irritating, often time-consuming problem. The greater speed and flexibility of cloud-assisted security enables more rapid update times, driving greater accuracy and reducing false positives.

No organization wants to dedicate their time to constantly compiling, revising and updating lists of acceptable, 'safe' applications. And what about printer drivers, networking software and essential updates? How do you make sure essential updates aren't incorrectly flagged as dangerous? Kaspersky Lab's Dynamic Whitelist looks after this for you. Produced by a dedicated Whitelisting lab, working with hundreds of international partners, it's essentially an enormous database of 'clean' software, continuously updated with information on file types, updates, installation files and – most importantly – information about them. There are approximately 1.5 billion files on Kaspersky Lab's database, to which Kaspersky Security Network has constant access.
A program classified as 'clean' today, may carry malicious code tomorrow – only constant monitoring and analysis can ensure reliable reputational information. Independent analysis by West Coast Labs found that Kaspersky Lab's cloud-based database contains data on 94% of all clean software released globally.
No security cloud is perfect; malicious files and URL can occasionally be incorrectly labelled as trusted/untrusted. In addition, it continuously analyses performance to improve quality.

INTRODUCING KASPERSKY PRIVATE SECURITY NETWORK FOR UNIQUE COMPLIANCE, SECURITY POLICIES AND TRUST REQUIREMENTS



The first image illustrates how Kaspersky Security Network works. The second image shows how Kaspersky Private Security Network operates entirely within the corporate infrastructure.

Now that you understand the benefits and functionality of KSN, let's take a look at how Kaspersky Private Security Network meets the needs of organizations with stringent data controls in place.

The first thing to remember is that, while KSN data is always completely anonymized, Kaspersky Private Security Network takes that level of security a step further by bring the cloud into the local premises, ensuring the organization retains complete control of all data while benefitting from threat intelligence gathered by KSN.

KASPERSKY PRIVATE SECURITY NETWORK: GLOBAL BENEFITS, LOCALLY DELIVERED

Kaspersky Private Security Network is installed in the organization's own data center; their own IT/security specialists retain complete control over it. Meanwhile all the security benefits – real-time threat analysis, reputation analysis, proactive threat detection, dynamic whitelisting – are available to the organization.

KPSN is particularly well suited to organizations with strict regulatory compliance, industrial or governmental standards in place. There is even an 'air-gap' deployment option available for network segments in which an Internet connection is not desirable.

While many vendors of cloud-assisted security offer 'caching proxies' that reduce the number of times a system has to contact the cloud for reputational data, Kaspersky Lab is unique in its ability to deploy the cloud entirely locally, within the organization's own data center and with zero outbound transactions with third-party servers. This capability is crucial in some industrial and governmental settings.

For added security, KPSN implementations retain local signature databases. Where some solutions completely migrate this capacity to the cloud, this leaves the customer exposed to attack while the migration takes place. With KPSN, this doesn't happen; during deployment, Kaspersky Lab's local databases (which can be updated manually) continue to provide optimal protection, eliminating any gap in security.

Once it's up and running, KPSN can become a source of unique threat intelligence and information for other solutions you may be running: security operation center, SIEM, risk management GRV, forensics and remediation processes...all can integrated with the data feeds, delivering unique insight into your organization's security and threat readiness.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab