▶ INTELLIGENCE SERVICES: THREAT DATA FEEDS

Protect your infrastructure from malware and dangerous URLs by leveraging Kaspersky Lab's comprehensive intelligence data.

Malware families and variations have grown exponentially in the last few years; Kaspersky Lab detects about 315,000 unique malware samples daily. To protect their endpoints from these threats, most organizations deploy classical protection measures like anti-malware solutions, intrusion prevention or threat detection systems. But how can countries defend national interests and infrastructures from significant volumes of malware – and the new techniques they use to bypass traditional and even more sophisticated protection measures?

The solution is for governments, telecommunication providers and other large organizations to block malware at the infrastructure level, using Threat data Feeds from Kaspersky Lab.

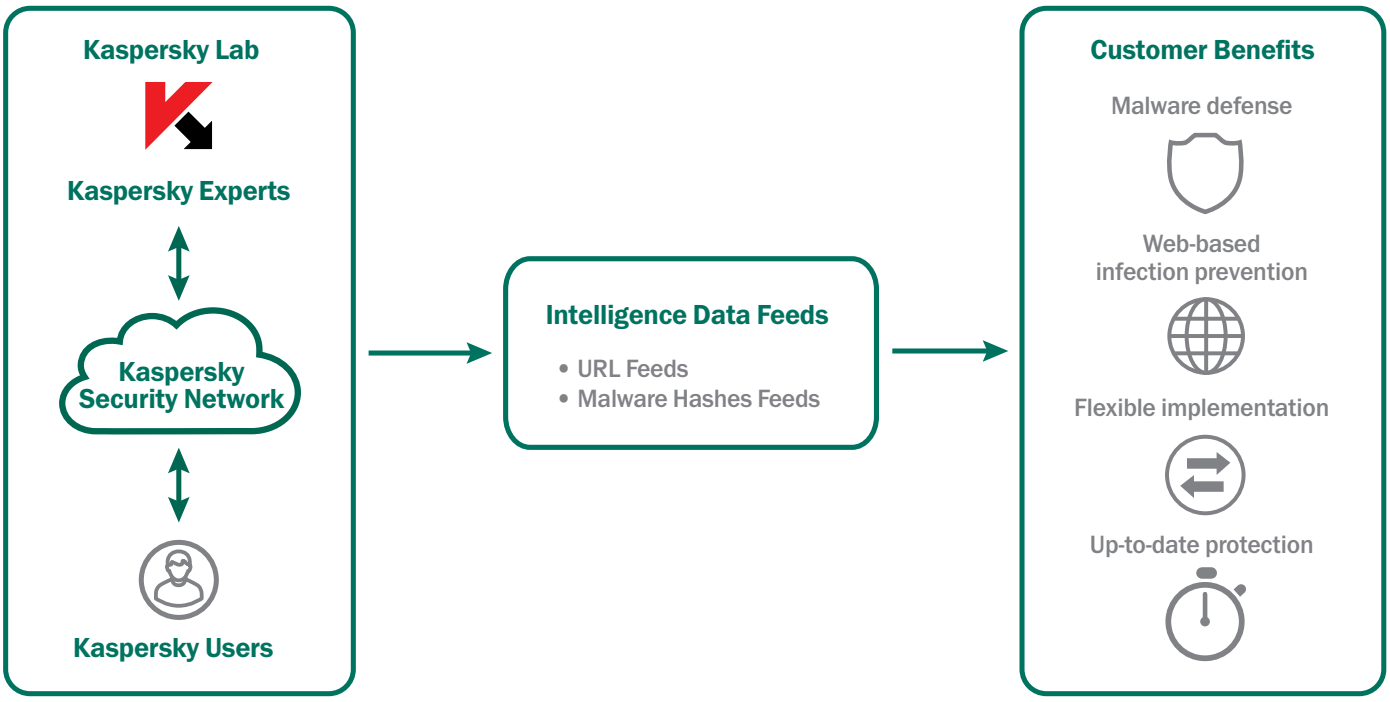
KASPERSKY'S THREAT DATA FEEDS CAN IMPROVE YOUR SECURITY POSTURE:

Malware defense – The distribution of malicious objects can be blocked at the infrastructure level by adding the MD5 message digest hashes to the blacklists of network level gateways and firewalls.

Web-based infection prevention – Malicious URLs can also be blocked by adding the URLs and corresponding masks into blacklists of network level gateways and firewalls.

Flexible – Intelligence Feed databases can be integrated into third party cyberthreat intelligence solutions.

Up to date – Intelligence Feed databases are updated regularly with the latest findings correlated from the cloud network and other sources.



Kaspersky lab offers two types of Threat data Feeds:
1. Malicious URLs and masks
2. MD5 hashes of malicious objects database

Feed Description
Malicious URLs — a set of URLs covering the most harmful links and websites. Masked and non-masked records are available
Phishing URLs — a set of URLs recognized by Kaspersky Lab as phishing. Masked and non-masked records are available
Botnet C&C URLs — a set of URLs of botnet command and control (C&C) servers and related malicious objects. Mobile C&C are included
Malware Hashes (ITW) — a set of file hashes covering the most dangerous in-the-wild malware encountered by Kaspersky Security Network users. The Base contains hashes with Kaspersky verdicts for each object
Malware Hashes (UDS) — a set of file hashes detected by Kaspersky cloud technologies (UDS - Urgent Detection System) based on a file's metadata and statistics (without having the object itself). It allows the system to identify malware that is not detected by other methods. This can also be described as "recently identified malware hashes"
HTML Script Hashes — a set of hashes of malicious scripts embedded into HTML pages with verdicts according to Kaspersky Lab classification. This base allows detection of scripts right after they are processed, without the need to download an entire HTML page to calculate its hash
Android Malware Hashes — a set of file hashes for detecting malicious objects that infect mobile Android platforms

For more information on Threat Data Feeds or other Kaspersky Services, please contact us via intelligence@kaspersky.com today!

WHY KASPERSKY LAB?

- Founded and led by the world's foremost security expert, Eugene Kaspersky
- Partnerships with global law enforcement agencies such as Interpol and CERTS
- Cloud-based tools monitoring millions of cyberthreats across the globe in real time
- Global teams analyzing and understanding Internet threats of all kinds
- World's largest independent security software company — focused on threat intelligence and technology leadership
- Undisputed leader in more independent malware detection tests than any other vendor
- Identified as a Leader by Gartner, Forrester and IDC

TO LEARN MORE VISIT: **WWW.KASPERSKY.COM**