Kaspersky Network Security Threat Data Feeds

kaspersky bring on the future

Endpoint protection alone isn't enough.

Network-level protection is also necessary.

Here's why:

- Protection from different types of attacks should consist of multiple layers
- Not all hosts in your environment will have endpoint security protection, e.g. not all business-critical servers, or hosts in an industrial network
- Some 'protected' hosts may not be up to date with signatures / hashes / detection rules

Kaspersky Network Security Threat Data Feeds

Almost every company these days has a Next-Generation Firewall (NGFW). It's one of the most effective modern network security controls, increasing the protection levels of corporate networks against cyberattacks.

The majority of NGFW are not only capable of utilizing internal knowledge about cyber threats, but also offer functionality that allows you to use dynamic lists of indicators of compromise (IoCs) from external sources to block cyberthreats in real time

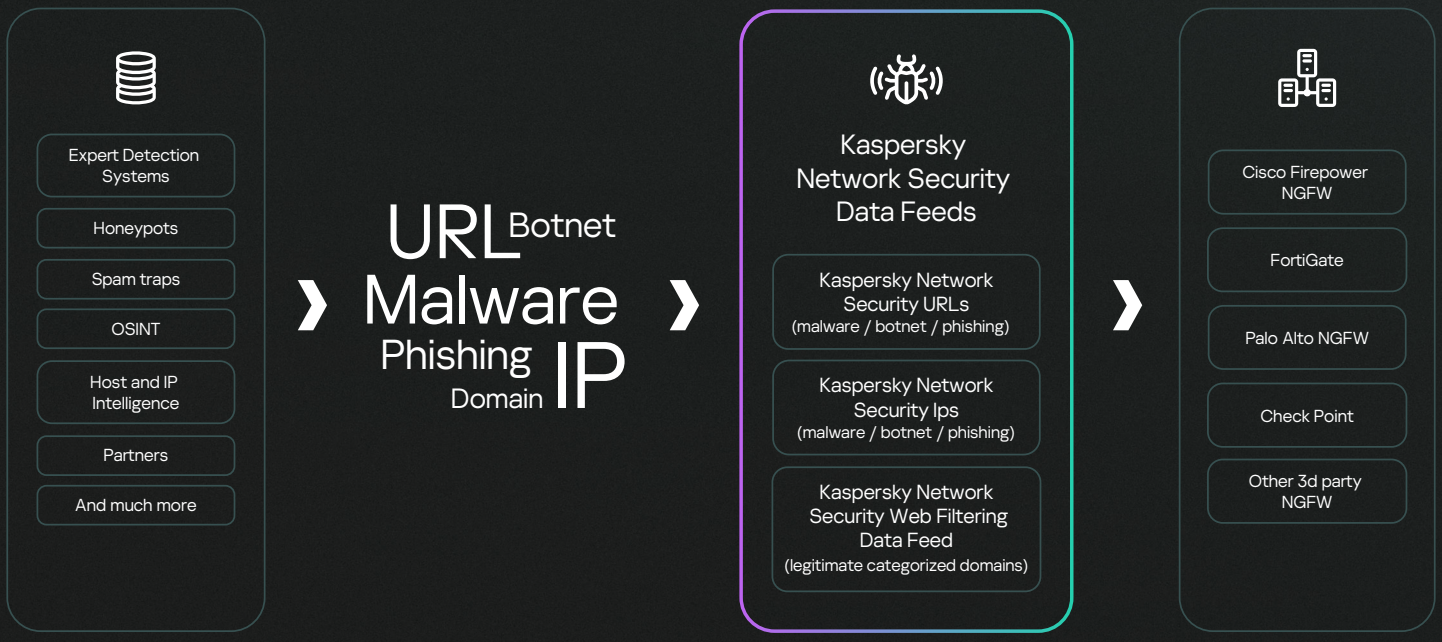
Having to quickly configure NGFW detection rules to always stay ahead of adversaries is almost impossible. This is why external threat intelligence knowledge is essential. It brings a critical extra element of protection to your environment which may otherwise be missed.

Kaspersky offers specially created collections of IoCs which, when imported into a NGFW, significantly improve the level of security protection of the corporate network from the most prevalent threats, without complicated integration or configuration, and retaining the current network topology.

Kaspersky Network Security Threat Data Feeds are based on Kaspersky Threat Intelligence Data Feeds and contain regularly updated lists of various types of IoCs (IP addresses and domains). Using this information enables you to monitor/block user access to dangerous network resources.

Learn more

Kaspersky Network Security Data Feeds Integrations



Data collection and processing

Kaspersky Network Security Data Feeds are comprised of multiple lists, each focusing on a specific type of cyberthreat. The feeds contain the lists of IP addresses with the highest threat score and top-level and second-level domains of resources which are known to distribute malware, act as botnet command and control centers (C&C) or host phishing resources.

Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network and our proactive web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), host and IP intelligence services.

All the aggregated data is carefully inspected in a real time and refined using multiple reprocessing techniques, such as statistical criteria, sandboxes, heuristics engines, similarity tools, behavior profiling, analyst validation and allowlisting verification.

Highlights

Real-time updates

Data Feeds are automatically generated in real time, based on findings across the globe to provide high detection rates and accuracy levels.

Kaspersky Security Network provides visibility into a significant percentage of all internet traffic, covering tens of millions of end-users in more than 213 countries

Native support

Native support for the most popular NGFWs:

- Cisco
- FortiGate
- Palo Alto
- Check Point
- Other 3d party NGFWs (with functionality of external dynamic lists with basic authentification support)

Secure authentication

Data Feeds offer a range of authentication methods tailored to meet different security needs and integration preferences

Easy integration

Supplementary step-by-step configuration guides for each supported NGFW and technical support from Kaspersky enable easy configuration and deliver immediate value

Continuous availability

All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability

100% vetted data

Data Feeds littered with false positives are harmful, as they can block legitimate resources.

Kaspersky Network Security Data Feeds apply extensive tests and filters are applied before releasing feeds, ensuring that 100% vetted data is delivered

Benefits

Reinforce your network defense solutions

with continuously updated IOCs to automatically block the most prevalent cyberthreats

Prevent the exfiltration of sensitive assets

and intellectual property from infected machines to outside your organization

Block cyberthreats fast to protect

your organization against cyberthreats and maintain business continuity

Kaspersky Threat Data Feeds

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture