



Kaspersky Anti-Virus SDK

Kaspersky Anti-Virus® Software Development Kit (KAV SDK) v.8 is the most reliable way to add anti-malware functionality to your software, hardware and IoT solutions.

Kaspersky Anti-Virus SDK v.8 is a set of development libraries enabling the integration of Kaspersky Anti-Virus engine into third-party hardware or software products as well as Internet of Things solutions (including smart routers, printers, and basically any other internet-enabled devices). SDK v.8's flexible and smart architecture and comprehensive API's allow implementing Kaspersky Anti-Virus technology into a variety of software and hardware platforms.

Kaspersky award-winning anti-malware technology empowers the SDK v.8 with unparalleled reliability and versatility.

Application Area

Third party vendors can use Kaspersky Anti-Virus SDK v.8 to enhance their products with comprehensive protection against:

- Viruses, Trojans, worms and all kinds of malware, spyware and adware
- Rootkits, bootkits and other complex threats
- Identity theft by keyloggers, screen capture malware
- Botnets, ransomware, crypto-mining malware, and other illegal methods of hijacking your endpoints
- Zero-day attacks and unknown threats, including many APTs
- Drive-by download infections
- And many other cyber-threats!

All-Round Support

- Dedicated technical and business account managers
- Qualified 24x7 technical support
- Marketing support
- Frequent anti-malware database updates

Attractive Licensing Scheme

- Flexible SLA
- Attractive business models
- Free upgrade to new versions

Key Benefits

Kaspersky Anti-Virus SDK v.8 embodies all the latest innovations from the Kaspersky Virus Lab. Now it is even faster, stronger and easier!

Perceive the **Speed of Kaspersky Anti-Virus SDK v8** with a new generation of the core anti-virus engine:

- Improved malware search algorithm, which is critical considering the rapid growth of the anti-virus database
- Improved operations with compressed objects, which contribute toward the increase of processing speed by eliminating unnecessary I/O operations
- Native multithreading support
- Optimized anti-virus database format consuming less RAM & disk space

Feel the **Power of Kaspersky Anti-Virus engine** with its optimized malware detection methods:

- AV Engine is updatable: by incorporating new detection technologies, procession logic including AV database format can be upgraded/ modified by means of regular AV database updates
- Detection of multipacked objects and objects packed using "grey" compression utilities (frequently used for hiding malicious programs from AV software)
- Advanced heuristics module
- Kaspersky Security Network that supplements the onsite technologies with additional immediate cloud-based detection.

Notice its **Easy and flexible integration**:

- Cross platform API (similar APIs for Linux/Unix and Windows versions)
- Two API sets: high level API for fast and seamless integration and low-level API set for deep and flexible integration

Recent Kaspersky Product Awards from Independent Testing Labs



...and more – for details see www.kaspersky.com/top3

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

©2024 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.

Protection Methods

- **Machine Learning Technologies.** Today Kaspersky analyzes 99.9% of the cyberthreats using its own proprietary infrastructural algorithms powered by machine learning which greatly helps to boost detection rate of both the existing and the next-generation scanning technologies.
- **24x7x365 Anti-Virus Laboratory.** Kaspersky anti-malware technology is supported by 24x7 human analysis. The combination of human analysis with latest anti-malware technologies such as advanced heuristics and automated AV engine updates provides supreme malware detection rate and ensures instant reaction to new threats.
- **Advanced Heuristics.** This module includes the heuristic analyzer that emulates the object's execution in a secure virtual environment and discovers suspicious actions of executed objects.
- **Signature Analysis.** A signature is a unique sequence of bytes that is specific to a piece of malicious code. Signature analysis, or a modification of it, was one of the first methods used in anti-virus engines to detect malware, but still remains relevant today.
- **Kaspersky Security Network (KSN)** technology 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. The globally distributed malware monitoring carried out by KSN makes it easy to respond quickly to new threats no matter where the sources and targets are located.
- **Greatest Number of Packers and Archives Supported.** Thorough unpacking of compressed objects is achieved through DeepUnpack technology, supporting the largest number of formats (about 3,000) including nested archives and packed formats, and makes possible the processing of multi-volume archives.

New Features of Anti-Virus SDK

The latest version of Kaspersky Anti-Virus SDK (KAV SDK) is 8.9. The following list describes the main advantages of KAV SDK 8.9 when compared to previous product versions.

- **New "Cloud mode".** Allows to reduce anti-malware bases' size when connected to KSN. Reduces antivirus bases drive space by half (i.e., ~100+ MB).
- **Trusted files scanning.** Very fast scanning of trusted files (such as .msu Microsoft update packages).
- **Updatable SSL libraries.** Allows to fix OpenSSL vulnerabilities via bases' updates, without updating the entire product.
- **Format Recognizer.** Improves scanning speed by allowing the user to skip certain file formats which are unlikely to contain malicious payloads (for example, pictures).
- **Deletion of Adware and Riskware.** Added detection of 'yellow' URLs which are not malicious per se but can be annoying or harmful if misused. This includes Adware and Riskware categories.
- **Scanning mode suitable for a sandbox.** Added a new scanning mode which includes a notification that the scanned object is appropriate for sending to a sandbox solution. This allows using it with any sandbox solution on the market without affecting product performance.
- **Calculate MD5 and SHA256 hashes of any scanned object.** Previously it was possible only for malicious objects detected by KAV SDK engine. Please note the system performance can be decreased if you choose to get the hash sums of scanned objects.
- **Bases update over https.** More secure updates.
- **Extended list of file formats to be scanned with KSN.** This list is now updatable via anti-malware base updates. This feature improves the detection rate.



Kaspersky
Technology
Alliances

Kaspersky technologies are available for integration into third party hardware and software security products and services. All solutions are backed by professional technological partnership support.

Learn more at www.kaspersky.com/oem