Kaspersky for Business

How Kaspersky Lab's Application Control stops threats

www.kaspersky.com
#truecybersecurity

How Kaspersky Lab's Application Control stops threats

Dealing with malicious attacks

Malicious code spreads via websites, social networks and email as well as vulnerabilities in applications. Cybercriminals target companies of all sizes to steal money and confidential information. Around 360,000 malicious programs emerge every day… In rapidly changing circumstances like these, signature-based methods are no longer sufficient, as they block only known malicious files. The number of attacks has become so numerous that blacklisting technologies alone cannot cope.

Modern technologies and control tools are used to enhance security against new malware:

- Startup control (including Whitelisting scenarios)
- Behavior analysis
- Machine learning
- Application isolation and privilege control
- Journaling application activities
- Protection from exploits
- Vulnerability management

There are pros and cons to all of these proactive technologies: improvements in the level of security often lead to an increase in resource consumption and false positives.

Not all solutions are created equal…

Many niche market players claim that the various proactive security technologies are a substitute for traditional signature-based analysis (blacklisting). This is unlikely to continue to be the case because of the high cost of deploying and supporting a new system – and because signature-based methods are still the most effective when it comes to combating known malware.

Having failed to develop their own effective technologies, some companies just buy a niche player's solution and combine it with their own technologies in a single product, managed from a centralized administrative console. But problems can arise when technologies with different origins fail to coordinate effectively. This can lead to system overload, incompatibilities and complicated settings and management of corporate IT security.

Kaspersky Lab has chosen a fundamentally different approach by developing its own Application Control, Privileges control (HIPS), Exploit Prevention, Remediation engine and Vulnerability monitor technologies and integrating them seamlessly with signature-based and behavior analysis in Kaspersky Endpoint Security for Business.

How does Kaspersky Lab's solution work?

Kaspersky Endpoint Security for Business provides multi-layered protection by checking an application before it executes and controlling it while it runs:

Layer 1. File Threat Protection, powered by Kaspersky Security Network (KSN) and machine learning technologies, intercepts file operations and checks the application against known malware before it executes. All known malware is handled at this stage.

Layer 2. Application Control applies local whitelisting or blacklisting rules which are created by an administrator. The component allows flexible adjustment of corporate protection with a variety of Default Allow or Default Deny scenarios. For a better applications categorization, Application Control can use the Dynamic Whitelisting Database developed by Kaspersky Lab by systemizing knowledge of legitimate software.

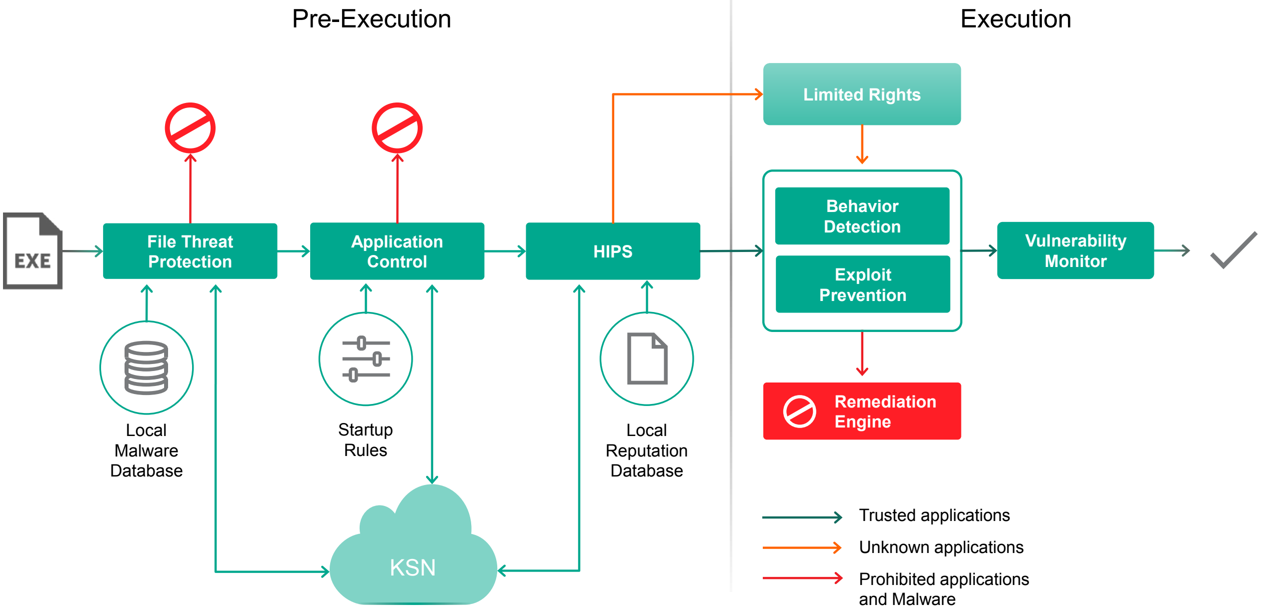
Layer 3. The last check before the application starts is performed by **Host Intrusion Prevention (HIPS)**. Based on local and cloud (KSN) reputations databases, **Host Intrusion Prevention** assigns every application to one of four default trust groups. Applications from the most trusted group are whitelisted and run without any limitations. The rest of the applications will run with limited privileges and limited access to critical system resources (depending on the trust group).

Layer 4. Finally, all running applications are subject to **Behavior Detection, Remediation Engine, Exploit Prevention** and **Vulnerability Monitor**. Behavior Detection and Exploit Prevention monitor application's behavior, block potentially malicious activity and protect whitelisted applications from being exploited and used by malware.

The Remediation Engine logs operations of applications which were not placed in the Trusted group. If an application turns out to be malicious, the Remediation Engine rolls back the actions.

The Vulnerability Monitor alerts about critical vulnerabilities, so that the administrator can install vulnerability fixes in time, update the application version or reduce its trust level.

How Kaspersky Endpoint Security for Windows Works



Protection components on every layer can work without Kaspersky Security Network (KSN). However, they are greatly enhanced by reputation and whitelisting services provided by Kaspersky Security Network. The dynamic Whitelisting reputation database in the cloud contains information about hundreds of millions applications. More than 80 million users of Kaspersky Lab cloud services and 700 global partners update the database regularly and promptly. It provides access to information about new software that is released every day, minimizing false positives.

Advantages of KSN whitelisting database:

The reputation base of Kaspersky Lab in the cloud contains information about more than 3 billion files and is continuously updated.

The dynamic Whitelisting database contains information about more than 300 million unique clean files and is growing by 1 million new files every day.

The status of applications already in the database is continuously tracked – the reaction to changes in an application's status is faster than that for other Whitelisting solutions due to all the technological infrastructure and expertise necessary for software analysis being concentrated within a single company.

Besides automated application scans, manual expertise is also used. The Virus Lab as well as the Whitelisting Lab, part of the Whitelisting & Cloud Infrastructure Research Department, constantly monitors database quality.

Information about software that is about to be released is received from more than 700 vendors, such as HP, Adobe, Intel, Asus, MSI, Mozilla and others, which helps minimize false positives.

Application Control

From the above components, all but Application Control work out of the box. Application Control must be enabled and configured by an administrator.

Application Control either allows or blocks files execution in accordance with the restriction policies set up by the administrator. Startup control implemented in Kaspersky Lab's solution allows highly flexible adjustment of protection and supports different operation modes:

- Blacklist (Default Allow) — all applications, except those explicitly prohibited by the administrator, are allowed to start. Non-business-related software such as games or videos can be blocked for all or some groups of users.

- Whitelist (Default Deny) — in this mode the administrator explicitly permits the use of some application categories and all others are automatically prohibited.

- Log only — a variation of Whitelist mode used to monitor execution of applications on machines where Default Deny cannot be implemented in blocking mode (because of constantly changing software or continuity requirements).

Application Control intercepts the launch of portable executable files (.exe .scr .dll) and also controls scripts executed by a variety of interpreters (.com .bat .cmd . ps1 .vbs .js .msi .msp .mst .ocx .appx .reg .jar .mmc .hta .sys).

Administrators can configure startup rules for applications based on the following criteria:

- Hash (SHA256)
- Certificate
- Kaspersky Lab categories
- Metadata (filename, manufacturer, version etc.)
- Path (or path mask)
- Device type
- User
- KSN reputation
- Application origin (creator of the application)

Kaspersky Lab categories is an in-house classification of applications provided by Kaspersky Lab. Application Control places applications to Kaspersky Lab categories using a combined mechanism that uses local rules enhanced with information from the cloud. Kaspersky Lab categories continue to work even when the computer is offline.

Tools for Whitelist mode

In the Blacklist mode the administrator can easily set up blocking rules using the criteria mentioned above. However, it's the Whitelist mode that benefits security the most. Application Control provides several tools to simplify the initial configuration of Whitelist rules:

- Predefined rules recommended by Kaspersky Lab
- Applications Inventory
- Wizard to create rules based on inventory results
- Dynamically updated whitelist rules based on Trusted Sources (file locations or reference computers).
- Kaspersky Lab categories to allow specific types of good applications known by KSN
- Wizard for creating rules based on events about blocked applications and applications prohibited in test mode

Handling unknown software

While setting up rules for Application Control in Whitelist mode it may be challenging to cover unknown software (without a digital signature) which is already present on protected machines. It's even harder to allow unknown software which is introduced in the system after Whitelist mode is already implemented. Recommended approaches to handling unknown software are as follows:

1. Use KSN to allow all known good applications.

2. Allow unknown software already present on computers by:
    - Hash-sums
    - Signing applications (using catalog file)
    - Putting unknown applications to a Trusted Source

3. Allow new unknown files using:
    - Trusted Updaters (covers software updates and applications that generate executable files)
    - Trusted User Accounts (covers installation of new software and execution of custom scripts)
    - Set up a procedure to place new files to a Trusted Source
    - Set up a procedure to sign new files
    - Process the rest of the files manually upon receiving User requests

Try True Cybersecurity for yourself

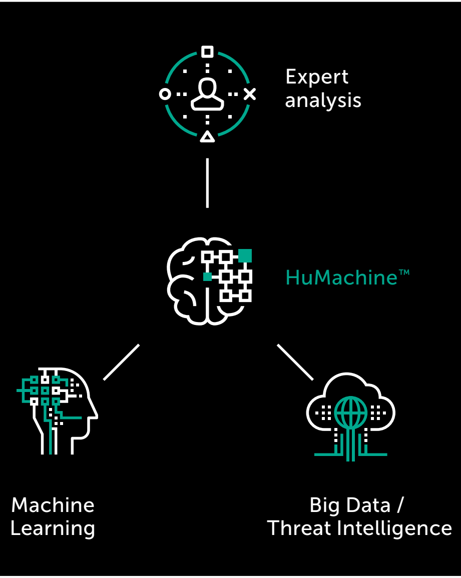
Experience for yourself how Kaspersky Lab combines ease-of-use agility with HuMachine™ intelligence to protect your business from every type of threat.

For a free, 30-day trial of the full version of Kaspersky Endpoint Security for Business, click here. At the end of the trial, if you decide to purchase, you just pay the license fees. As the application has already been running on your endpoints during the trial, there'll be nothing more for you to do.

Kaspersky Lab
Find a partner near you: www.kaspersky.com/buyoffline
Kaspersky for Business: www.kaspersky.com/business
IT Security News: business.kaspersky.com/
Our unique approach: www.kaspersky.com/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.com


Expert analysis
HuMachine™
Machine Learning
Big Data / Threat Intelligence