# Host-based Intrusion Prevention System (HIPS)

Kaspersky Internet Security consumer security solution features **Host**-based **Intrusion Prevention System** (HIPS). This system is designed to detect unwanted and malicious program activity and block it in real-time. Advanced Kaspersky Lab technologies enable HIPS responses to only be initiated for dangerous and unwanted events without affecting the operation of safe programs. This ensures a high level of protection for users with low consumption of the computer resources.

## Why do you need HIPS?

Today's computer users are faced with an ever-increasing number of malicious programs. Trojans, worms and viruses damage computer systems and communication channels, steal confidential data and spy on users.

Users need effective protection from hacker and malware attacks. Network Intrusion Detection Systems (NIDS) that analyze Internet traffic and internal networks are available, though their usefulness is limited due to the frequent use of data encryption on the Web. They also fail to protect against threats emanating from removable storage media. A system that can prevent attacks at the computer level (HIPS) is a more practical solution because it can monitor applications functioning on a specific PC and block any unwanted activity.

HIPS effectively combats:

- New threats before antivirus databases are updated, as it reduces the likelihood of intrusion and an infection being spread;
- Known threats, as it prevents them from launching;
- Suspicious applications, as it blocks dangerous activity;
- Theft of confidential data.

## Effective filtering of application activity

HIPS is, first and foremost, designed to filter application activity. The HIPS system implemented in Kaspersky Internet Security ensures close control over applications, restricting dangerous programs without affecting the operation of safe programs. Threats are blocked as soon as they appear on the user's computer, ensuring a high level of protection.

Following a detailed analysis, HIPS arranges launched applications according to reliability. The results from several technologies are considered:

- Anti-virus scanning;
- Search for a program in databases of trusted and untrusted software;
- Checks of digital signatures;
- Emulation (monitoring suspicious activity while imitating execution in safe mode);
- Comparing program behavior with the behavioral patterns of malicious programs;

The analysis of applications involves several criteria, enabling well-grounded decisions to be made regarding the level of danger posed. Because HIPS is capable of analyzing program behavior and the structure of program files, it not only combats known threats but also new malware whose signatures have not yet been included in antivirus databases.

Thanks to integration with Whitelisting, a service that lists trusted applications, HIPS is able to use any relevant data about safe programs. This makes it possible to minimize the number of false positives generated by legitimate software and means Kaspersky Lab products are even more convenient to use.

The flexible HIPS settings can limit activity by programs that have been analyzed – ranging from minor limitations to being blocked completely. Applications can be rated in accordance with four groups of trust: “Trusted”, “Low Restricted”, “High Restricted” and “Untrusted”. Applications in the Low Restricted or High Restricted groups are not considered malicious but have limited access to executable and non-executable files, the system registry, network and other resources.

Apart from assigning groups, HIPS enables a protection level for certain computer system objects to be configured. In other words, HIPS can be used to regulate access to certain objects by programs. For instance, it is possible to create a specially protected group of files to ensure complete protection of confidential data (banking data, e-mail, instant messaging) from theft.

As a result, the HIPS system implemented in Kaspersky Lab products filters application activity with greater accuracy and flexibility than systems where software is rated only as “white” or “black”.

## Easy to use for both advanced and novice users

When it comes to controlling application activity, Kaspersky Lab products satisfy a wide variety of user needs.

The user has the option of choosing the most suitable work mode:

- Interactive: when the user gives instructions to control application activity and the technology constantly adapts to specific user preferences (suitable for advanced users)
- Automatic: when all HIPS decisions are made without user input (suitable for less experienced users).

The user can change the preset rules for application activity control and protected resources as well as create additional personal resources and rules to control access to them. Moreover, the user can alter the limitations of a child application inherited from a parent program. For example, it is possible to label a program launched from an unknown version of an instant messenger as “Trusted”.

HIPS also enables the order of user activity requests to be configured in specific situations linked to application activity.

## The advantages of Kaspersky Lab’s implementation of HIPS

In conclusion, it should be noted once again that Kaspersky Lab’s HIPS technology has several unique functions which single it out from the range of similar methods for detecting malicious software implemented by other antivirus vendors.

- When an application is launched for the first time, HIPS analyses it in detail in order to assign it to a group. When it is subsequently launched, the object is check for continuity. If it has been modified, HIPS will perform another detailed analysis.
- If Internet access is available, the product receives information about a launched application from Kaspersky Security Network, the online reputation service. If the corresponding information has been updated, the mechanism that assigns the security rating group reassesses the application’s group. For example, if information about a previously unknown malicious program appears in the blacklist, it will be blocked completely.
- Moreover, the Urgent Detection System enables Kaspersky Internet Security 2010 to react promptly to new threats before antivirus databases are updated.

HIPS employs integrated technologies such as antivirus scanning, scanning using offline and online software databases, digital signature scans and security rating based on emulation and heuristic rules.