Kaspersky Enterprise Cybersecurity

The protection technologies of Kaspersky Endpoint Security

www.kaspersky.com
#truecybersecurity

The protection technologies of Kaspersky Endpoint Security

In this article we look at the threat detection technologies used in Kaspersky Endpoint Security – Kaspersky Lab's solution for corporate network endpoints.

Development history of endpoint protection

In the past, the endpoint concept only extended to workstations and servers; today it has expanded to include mobile devices as well as virtual environments. IT infrastructures have become more complex and taken on much more important roles in maintaining the operation of continuous processes.

Big data analysis, distributed storage of data, automation of processes – all of these require modern approaches to providing security. At the same time, confidential data and financial assets are attracting more and more attention from cybercriminals. Most of today's threats are essentially tools to make money, causing their victims substantial financial and reputational losses.

Complex attacks pose a new challenge to the developers of IT security solutions, and providing effective protection against them requires substantial expertise.

Workstations continue to be the main entry point for threats, and their need for quality protection continues to grow.

Below is a list of attributes that modern endpoint protection must possess:

- minimum impact on the target system resulting from the balanced operation of the technologies involved;
- prompt detection: advanced methods for detecting anomalous activities, including the use of expert cloud services;
- automated investigation of detected incidents;
- automatic rollback of malicious actions in the system;
- transfer of information about incidents into an SIEM event correlation system and other solutions;
- easy management: an intuitive interface with preconfigured functionality;
- centralized management;
- integrity control of internal protection technologies;
- effective services: product support, investigation research, training, etc.

It is evident from the above list that modern protection is no longer just a simple signature-based detection mechanism; it is a range of sophisticated technologies that makes easy management all the more important.

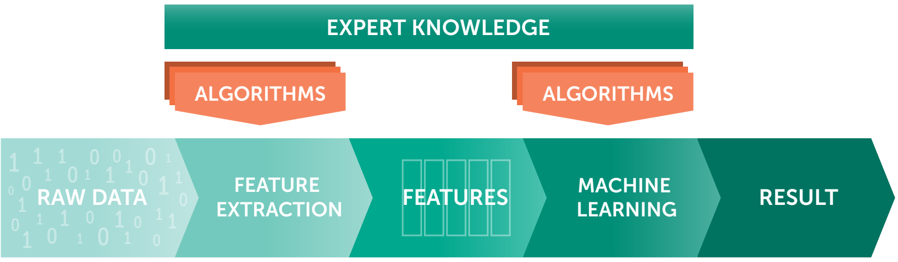
When choosing security tools, there are important factors to consider besides the functional requirements. It should be clear which technologies are applied within the solution, and how they are connected to each other. It is just as important to evaluate the manufacturer's level of expertise and experience and to assess its ability to continue developing technologies in the future.

Technologies involving machine learning

Feature engineering techniques are a process of applying expert knowledge to determine the attributes to be used in ML algorithms.

Machine learning (ML) methods have gained huge traction of late and ML has been successfully used with large volumes of data. However, it takes a significant amount of experience and expertise in IT security, combined with feature engineering techniques, before ML can be used effectively in threat detection.

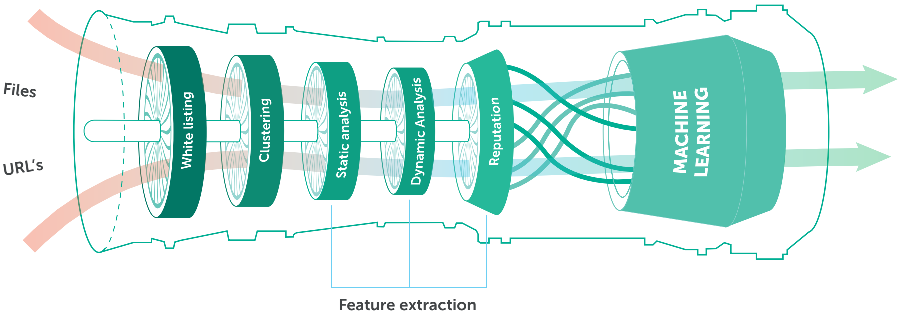
There is a common misconception that ML can be used with raw data in threat detection tasks. This is not exactly the case. As the old programming adage goes: "garbage in, garbage out." When arranging the training process, it is crucial that data is properly pre-processed and supplemented with expert knowledge (feature engineering). It would be naïve to think that effective algorithms can be built without malware analysts and their extensive expertise. Essentially, analysts play a supervisory role – they control and fine tune the work of algorithms, and get involved to verify the most complex threats for which automatic analysis may not always be sufficient.



Twenty years of development by its own research departments as well as analysis and accumulated expert data means Kaspersky Lab automatically detects the vast majority of threats using machine learning methods.

The threat processing and analysis center can be depicted as a ‘turbine’ that accepts objects as input; these objects undergo several stages of processing and analysis using various technologies, including ML algorithms. The resulting output analysis is used to formulate threat detection rules that are made available to users via Kaspersky Security Network.

Automated threat processing and analysis center



ML algorithms detect and define more than **310,000** unique threats each day. Thanks to the work of Kaspersky Security Network, most of these are made immediately available to endpoint security technologies.

At the same time, there is a real focus on preventing false positives. This involves newly created detection rules being checked against an extensive database of clean files.

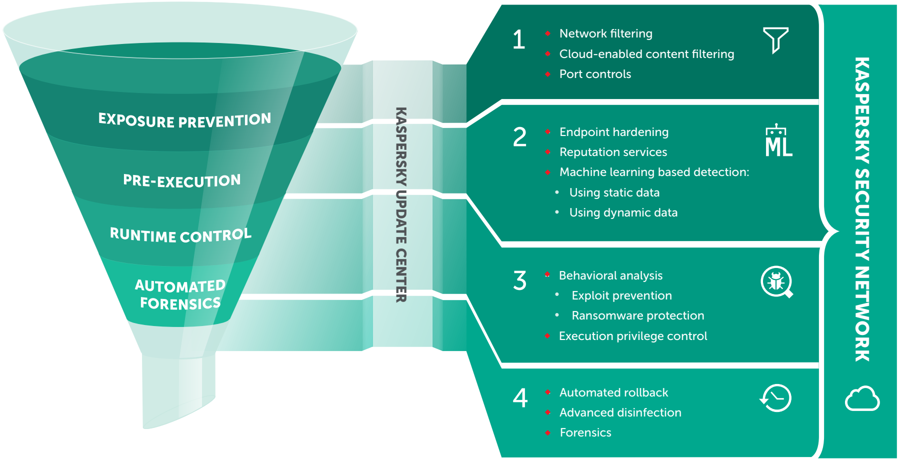
Kaspersky Endpoint Security

The evolution of threats targeting businesses has given rise to the emergence of a new generation of endpoint security technologies. Kaspersky Lab has developed and implemented various security technologies, including those using ML methods. With these technologies, Kaspersky Lab was able to dramatically speed up threat detection and, simultaneously, lower the overall footprint on the protected system. Today, Kaspersky Endpoint Security (KES) is a highly effective security product that protects endpoints in corporate networks.

Sequence of protection technologies

The logic behind KES operation can be loosely divided into four stages:

The Sequence of Kaspersky Endpoint Security Protection Technologies

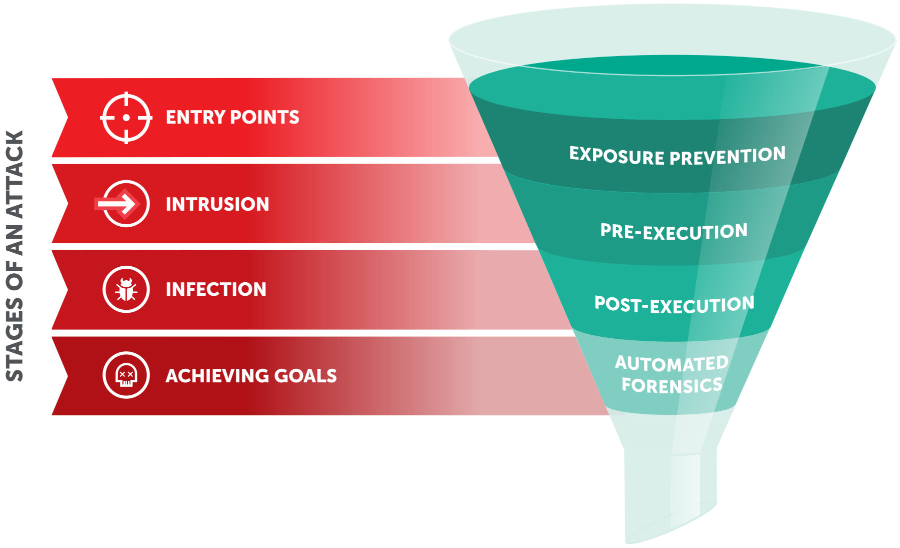


Each stage is represented by a group of stand-alone protection technologies. This means that each of the technologies is capable of detecting and blocking a threat that falls within its competence, whereas the above sequence of stages demonstrates the entire solution's capabilities. Along with security technologies, there are also two cloud services of expert support.

- The **update center** contains timely incremental updates of protection components, including local expert databases (such as the signature database, heuristic database, behavior scenarios database, etc.). Also, the update center accumulates the operational changes in the parameters of all ML algorithms used, enabling greater flexibility when providing protection.

- **Kaspersky Security Network** is a cloud-based infrastructure which provides real-time access to various statistical data (including reputation, content, behavioral, etc. statistics). This reduces threat detection times and conserves the resources of the protected node.

The above sequence of protection technologies is a response to the phases of an attack: each stage provides its own security level required to prevent a threat.



We will now look at each stage of the protection technologies individually.

1. Exposure prevention

Nowadays, threats spread via all possible information channels, and it is extremely important for a protected node's perimeter to be reliably protected.

The first stage is a filter for all incoming information. Preventive blocking technologies are used to monitor the main activity of the protected node, allowing early detection and blocking of known threats. Let's look at the blocking technologies of the first stage.

1.1 Protection from network attacks and firewall

The security of network connections is controlled by the **Intrusion Detection System (IDS)**, which is a signature-based network sensor. During operation, IDS applies the technology of Deep Packet Inspection (DPI), allowing the network sensor to control all passing traffic. This means it can promptly detect multiple suspicious and dangerous network events.

Some examples of network events are:

- active scanning of ports;
- attempts to connect to different ports of the operating system;
- detection of abnormal network communication, e.g. use of remote management tools, commands sent from a C&C (in cases involving botnets).

When a dangerous network event is detected, the sensor blocks the connection using firewall functionality.

Firewall – a blocking technology that filters the network activity of the protected node according to preset rules on:

- filtration of network packets and data streams;
- software activity when interacting with the network.

The parameters are set by the administrator in the network connection policy.

1.2 Web filtering

In 2016, 31.9% of user computers were subjected to one or more web attacks by malware-class malicious objects while using the Internet.

Internet resources are one source of threats. A trusted web node can be compromised and a malicious script or a 0-day exploit may end up being hosted on it, making everyday operations insecure. To ensure convenient, secure work with Internet resources, web filtering technology is applied in KES that consists of two protection levels.

The first level is associated with the cloud-based Kaspersky Security Network (**KSN**), and is responsible for passive filtration, i.e. it provides a real-time reference as to which category a web resource belongs to, or what reputation it has; this is done before the browser begins to download the content.

The KSN reputation database classifies URLs into the following categories:

- malicious URL – poses an infection hazard;
- phishing URL – is used for stealing personal information;
- unknown URL – no reputation information available;
- secure URL – safe resource.

Web filtering substantially contributes to security, blocks most websites known to be dangerous and conserves the resources of a protected node.

In 2016, 261,774,932 unique URLs triggered protection technologies.

The second level is based on the technology of dynamic analysis and tracks content downloaded from all unknown web resources. More details will be given when the second stage protection technologies are described below.

1.3 Control over connected peripherals

Portable devices also pose a potential threat to the protected node. Peripheral control identifies the type of device connected, and prompts the user to confirm that it is OK to connect the device – confirmation requires the user to enter the key that is displayed. This control helps identify cases of spoofing, e.g. when a memory card masquerades as a keyboard to avoid scanning. Cybercriminals use this method to trick security technologies and penetrate the protected perimeter. Peripheral control is inextricably connected to the technologies at the execution prevention stage, where unknown objects are analyzed.

2. Execution prevention stage

For cybercriminals, it is important not only to bypass initial filtering but also to trick the detection technologies responsible for early identification of malware. An infection can only be considered successful when the malicious code is allowed to run within the trusted environment. To achieve that, cybercriminals are continually improving their techniques for bypassing detection technologies. The main techniques are listed below:

- **packers** – contain the malicious body in a packed form, thus complicating its detection;
- **code obfuscation** – used by special compilers to complicate the code at the algorithm level;
- **polymorphism** – when a malicious program's code is modified while it is being executed;
- **server polymorphism** – when a new sample of a malicious program is generated by a malicious server every time the server is accessed;
- **encryption** – multi-level encryption is used to conceal part of the code from detection mechanisms. Often used together with obfuscation;
- **vulnerabilities, including 0-days** – exploiting software vulnerabilities is an effective infection method;
- **bypassing emulators** – an anti-malware emulator checks an executable file by running it in an isolated environment and analyzing its logic of operation. Malicious code can be detected using signatures or heuristically. Hackers use different methods of modifying the code's algorithm to prevent the emulator from determining its logic.

Using two or more of the above methods in combination is a powerful cybercriminal practice, often used to penetrate the environment of a protected node. The only way to counter this is to use comprehensive technological protection that comes with the latest methods for controlling and analyzing executable objects.

The execution prevention stage is among the busiest, with a huge amount of objects being continuously analyzed.

Let us take a detailed look at the technologies that this stage is based on and the tasks that are performed.

2.1 Reinforcing the trusted environment

First and foremost, control is enforced over the trusted environment. This is done to mitigate potential threats by tracking down and eliminating vulnerable components in the operating system and third-party software.

To do this, a vulnerability assessment is run, which uses the global CVE (Common Vulnerabilities and Exposures) database. This is an automated process that is centrally managed by the Kaspersky System Management component. It helps to promptly report threats identified in software, and eliminate them in a timely manner with the help of the Patch Management software update technology.

According to detection statistics for 2016, software vulnerabilities are actively used as infection points.

The software update technology helps keep installed software up to date. When used in combination, the two technologies reinforce the protected environment and substantially reduce the possibility of vulnerabilities being exploited.

It is also important to note the additional **Default Deny** blocking technology. It implements an alternative approach to software launch control, which is basically "if it's not allowed, it's prohibited".

As part of the efforts to improve the quality of threat detection and minimize false positives, Kaspersky Lab is advancing the Technology Alliance, which includes TOP-500 software manufacturers as well as independent freeware developers. This way, Kaspersky Lab can proactively generate white lists, including those that can be used with Default Deny technology.

With this approach, the administrator can specify which software products are required and sufficient to carry out the company's operations.

The advantages of the Default Deny approach are as follows:

- unknown applications can be blocked, including new modifications of malicious programs;
- the installation and launch of illegitimate/unlicensed software that is not related to work tasks can be blocked.

This technology provides a broad range of categories that the administrator can assign to software programs (e.g. trusted manufacturers, trusted accounts added manually, unauthorized or unlicensed software, etc.). The lists are generated and updated automatically by the threat processing and analysis center, and do not require human involvement.

2.2 Reputation services

This part of Kaspersky Security Network ensures that threats are detected promptly; this is done with the help of online reputation databases containing detailed information about objects. The databases are continuously replenished with expert information, which includes information arriving from the detection technologies owned by other KSN infrastructure participants using the expert cloud for protection. The advantages of these reputation services are as follows:

- verdicts are issued instantly for each object;
- do not rely on the endpoint's computing resources.

After checking, each file is assigned a category:

- **Malicious** – file contains malicious code;

- **Clean** – file has passed analysis and was recognized as secure;

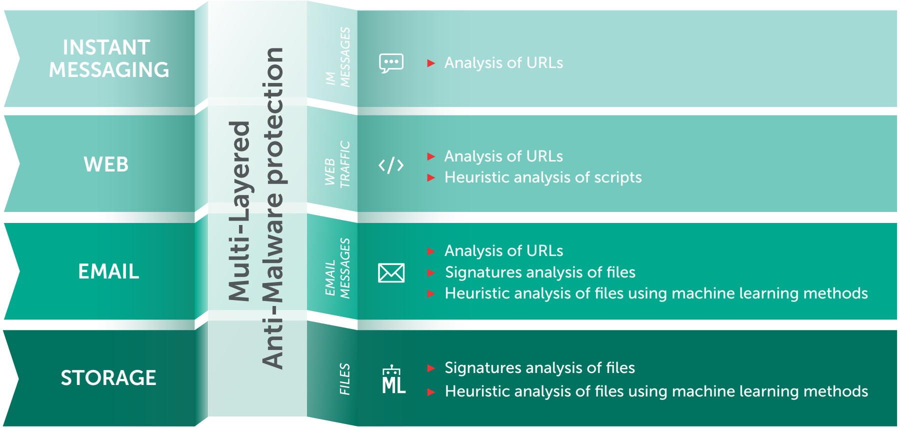
- **Unknown** – a new file that has not been analyzed before, and is potentially dangerous.

Each file classified as 'Unknown' is automatically passed for analysis to detection technologies that use machine learning (see below).

2.3 Multi-tiered protection

The final task in the second stage is to identify complex threats by employing different analysis technologies. This is done using a multi-tier protection component that consists of a set of scenarios predetermined by the type of information entry point.

Multi-tiered protection works as follows:


INSTANT MESSAGING
WEB
EMAIL
STORAGE
Multi-Layered Anti-Malware protection
IM MESSAGES
WEB TRAFFIC
EMAIL MESSAGES
FILES
ML
▸ Analysis of URLs
▸ Analysis of URLs
▸ Heuristic analysis of scripts
▸ Analysis of URLs
▸ Signatures analysis of files
▸ Heuristic analysis of files using machine learning methods
▸ Signatures analysis of files
▸ Heuristic analysis of files using machine learning methods

Each scenario has its own set of assigned detection technologies; however, when required, the detection technologies can be used in combination, which will ensure the required level of protection.

Web filtering – dynamic protection

Let us begin with a technology that operates as a continuation of Web filtering (an initial filtering stage). It is responsible for the active phase of threat detection in the downloaded content. At the initial stage, URLs are statically controlled to define the specific category each web resource belongs to; at the second stage, unknown HTML code undergoes dynamic analysis as soon as its controlled download begins.

The following technologies are applied at the active stage of detection.

- **Heuristic URL analysis**
  Each URL is analyzed at the moment it is opened in the browser on the protected node. The HTML code is loaded into an emulator, and its execution is monitored by a heuristic analyzer. This helps identify threats hidden in the HTML code, making it possible to block dangerous web resources from opening.

- **Heuristic analysis of scripts**
  Special attention is paid to the analysis of scripts in HTML documents. This involves the additional use of an emulator capable of detecting complex threats in different script languages. The passive (initial filtration stage) and active (intrusion prevention) levels of **Web filtering**, used in combination, ensure a secure browsing experience for the user.

  Web filtering technologies are also applied in security controls when working with any other information entry points where a URL address may be present, e.g. in **email or messengers**.

2016 statistics: web filtering technologies detected 69,277,289 unique objects, such as scripts, exploits, executables, etc.

Email

When analyzing email for threats, as well as **URL heuristic analysis**, some additional technologies are applied to analyze file attachments.

Email is one of the exposure points most exploited by cybercriminals. There is an entire trend in social engineering called spear phishing, which is an approach designed to have a carefully targeted impact. For instance, a specially crafted email may be sent to the target user containing an exploit along with archived attachments; the passwords to the archives may be provided in the body of the message or in graphical form. This imposes certain requirements on protection tools, namely, the ability to automatically open and analyze archived files.

Let’s now turn to the technologies of file analysis.

- **Signature-based file analysis**
  The technology of signature-based analysis is applied in different protection scenarios where an object needs to be checked fast for the presence of a threat. In the email scenario, it is needed for checking attached files.

  The signature-based method has certain advantages; this is why it is applied first for file analysis. Its main advantages are:
  - fast detection;
  - minimal level of false positives;
  - little demand on the protected node’s resources.

  This method is naturally limited by the number of signatures existing in the database (which is continuously updated). For this reason, the signature-based analysis works in combination with heuristic analysis.

A signature is a fragment of code that unambiguously identifies a malicious object.

- **File analysis using machine learning methods**
  Below, we will take a detailed look at file analysis using machine learning. In an email protection scenario, machine learning provides the unique capability of unpacking password-protected archive attachments. To do so, it extracts the password from the body of the message (which is either in graphic or text format). This is one of the techniques used by cybercriminals to bypass detection technologies: the protected archive acts as a ‘safe’, the contents of which are unavailable for analysis. To recognize the password provided in graphic format, a machine learning algorithm is employed. After this, the password is used to extract the contents of the password-protected archive.

File Storage

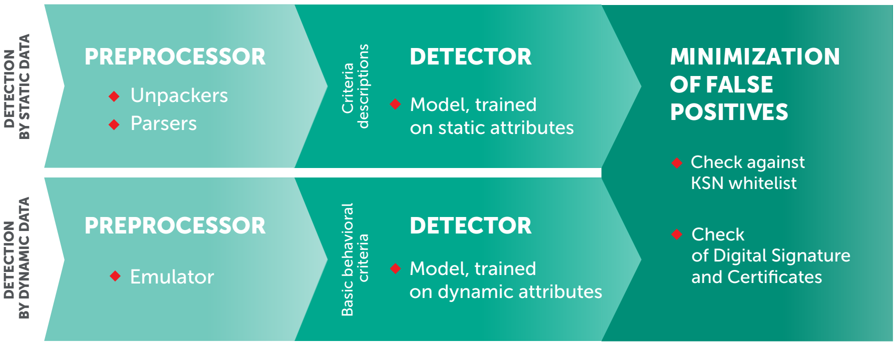
Each unknown file poses a potential threat to the protected node, and requires special attention from protection technologies.

For such cases multi-tier protection has an advanced scenario in which a deep analysis is run, employing machine learning methods.

There are several file analysis technologies.

- **Signature-based file analysis**
  The main advantages were listed above, in the email security section. In this scenario, signature-based technology plays the role of a basic filter – it provides verdicts for all known files, and leaves only unknown files to be analyzed using machine learning methods.

- **File analysis using machine learning methods**
  This is the most advanced technology in multi-tier protection. It runs a deep analysis of files, so threats can be detected early. This technology is based on the execution of two parallel processes that perform file analysis on static and dynamic data.


DETECTION BY STATIC DATA
PREPROCESSOR
Unpackers
Parsers
Criteria descriptions
DETECTOR
Model, trained on static attributes
MINIMIZATION OF FALSE POSITIVES
Check against KSN whitelist
Check of Digital Signature and Certificates
DETECTION BY DYNAMIC DATA
PREPROCESSOR
Emulator
Basic behavioral criteria
DETECTOR
Model, trained on dynamic attributes

These two processes fall into three stages, each stage consisting of specific groups of technologies. The static and dynamic approaches work well in combination and compensate for each other's potential shortcomings, such as:
- when the model is trained on static attributes of malicious programs, some files may appear that differ only slightly from clean files;
- when the model is trained on dynamic attributes, some programs may fail to demonstrate malicious behavior – they may require a specific environment or a dedicated command line for launching.

Further on, we will take a closer look at how each process works.

Static data is information about an object that is collected without executing it. This technology has a high generalization capacity and performance.

Detection based on static data

Preprocessor, preparatory technologies:

- **unpackers** extract packed code, and allow parsers to extract metadata from it (packers, obfuscation and encryption are typical detection evasion methods used by cybercriminals);

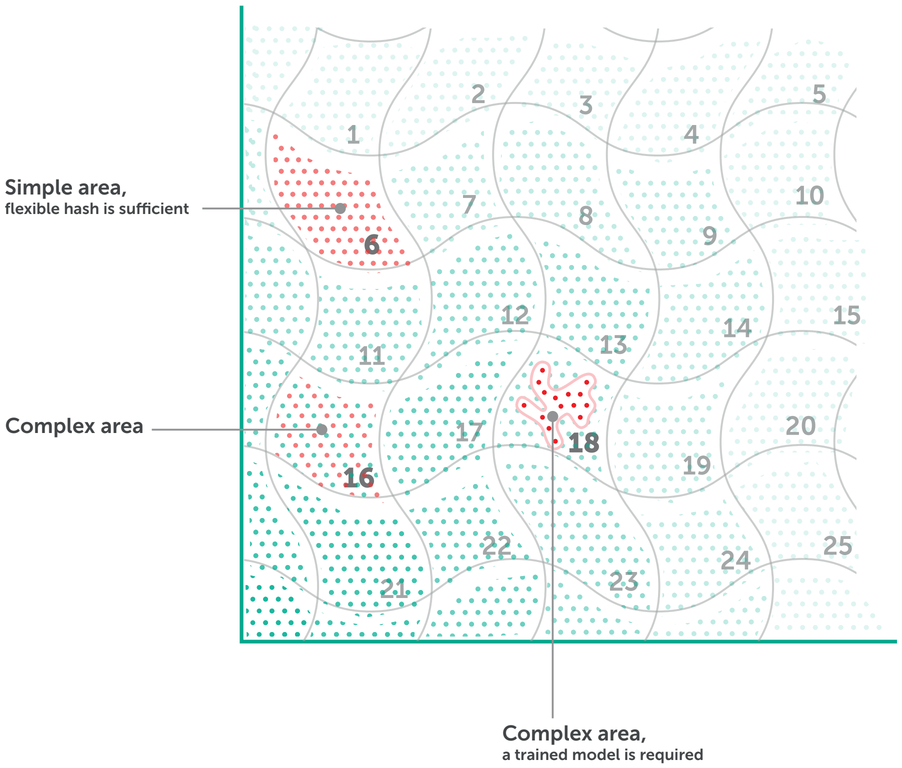
- **parsers** – tools for extracting various sets of metadata.

The diversity of metadata directly impacts the quality of detection, so the preprocessor contains a large library of different parsers. The parsers provide informative attribute descriptions (such as the structures of executable files, statistical characteristics of data and code, strings, etc.)

The **detector** analyzes attribute descriptions and passes a decision about whether each analyzed object is malicious or not. The detector's operation falls into two stages.

At the first stage, a flexible hash is calculated, making it possible to effectively check for the presence of the analyzed object in the 'dirty' area. If the area is simple (i.e. it only contains objects of one type – either all 'clean' or all 'dirty'), the verdict can be issued at this stage. A flexible hash has the advantage of being tolerant to polymorphism and obfuscation, substantially reducing the amount of resources required on the protected node.

Space of objects



The flexible hash is built based on attributes in such a way that it is the same for a group of files.

An area is part of the space of objects to which a flexible hash or a trained model corresponds.

If the area is complex (i.e. it contains both ‘dirty’ and ‘clean’ objects), the object is forwarded to the second stage for analysis. At the second stage, the object’s attribute descriptions are assessed by the classifier, whose job it is to find and apply an appropriate trained model (specializing in that specific area) out of the many models contained in the database. The trained model generates the final decision on whether the object is malicious or not.

Object analysis based on dynamic data

The **preprocessor** collects dynamic information, such as the object’s behavior, memory areas containing executable code, etc.

Dynamic data is information about an object, including information about its behavior collected while it is executed or its execution is emulated.

The emulator makes it possible to run an executable file in a controlled environment which partially imitates the actual system. Its advantages are that it has minimal impact on computer resources and security (the analyzed code cannot impact the trusted environment). Dynamic analysis produces a recorded sequence of the actions of the executed file, as well as a memory dump and other objects (e.g. files) which were generated during its execution. All the listed data constitutes basic behavior attributes.

The memory dump makes it possible to gain access to the original (unpacked) code, and detect data that may point to the malicious nature of the file.

The **detector** identifies malicious behavior scenarios and makes a decision on whether each analyzed object is malicious or not.

The detector uses a library of malicious scenarios which is created by Kaspersky Lab’s automated center for threat processing and analysis.

A malicious scenario is a sequence of actions through which an attack is implemented.

2016 statistics: multi-tiered protection reported 4,071,588 unique malicious and potentially unwanted objects.

The center has large collections of malicious and clean files which it continuously processes, extracting basic behavior attributes that are used to train models. The models transform into behavior scenarios and are delivered to the detector in the form of incremental updates. This approach dramatically reduces the time required and the size of the update, thus maintaining effective operation of the detector.

A false positive is an erroneous verdict passed by the detector stating that an object is malicious, though the object is in fact clean.

Minimization of false positives

Each decision passed by the detector is checked for a false positive. The occurrence of a false positive is a very low probability event; however, if it does occur, it can lead to grave consequences.

When an object is detected as malicious, the following minimum checks are run to reduce the risk of a false positive:

- a request is sent to the KSN cloud service, indicating the number of the trained model or behavior scenario that issued the decision about the identified threat. (KSN contains information about valid models and behavior scenarios, so it can check whether the model/scenario has been recalled.)
- a request is sent to the KSN cloud service's white lists, so any false positives from the detector can be ruled out. (White lists are a large collection of files known to be clean. This collection is constantly updated by Kaspersky Lab's automated center.)
- a request is sent to a certificate classification cloud service to check the reputation of the certificate used to sign the file.

With regards to the second stage, it is important to note that there is a local KSN cache that helps prevent repeated requests about objects that were already checked, thus conserving the resources of the protected node.

In 2016, cryptor attacks were blocked on the computers of 1,445,434 unique users.

In 2016, Kaspersky Lab detected more than 54,000 new modifications and 62 new families of cryptors.

3. Execution control

Although the second stage includes static and dynamic analysis, some threats may still pass this stage undetected. For example, multi-component cryptors that use legitimate encryption software may fly under the radar, as each individual component does not pose a threat.

The aim of the third stage is to detect malicious behavior within the trusted environment. During analysis, the overall behavior of all active components is taken into account, including that of trusted and non-trusted applications, as well as of system components. This sort of analysis helps identify complex, multi-component threats.

0-day vulnerabilities are errors in the code that have yet to be patched, allowing a cybercriminal to use undocumented program execution features to compromise the system.

Behavior analysis looks at the actual behavior rather than at the presumed (emulated) picture of actions that is analyzed at the intrusion prevention stage.

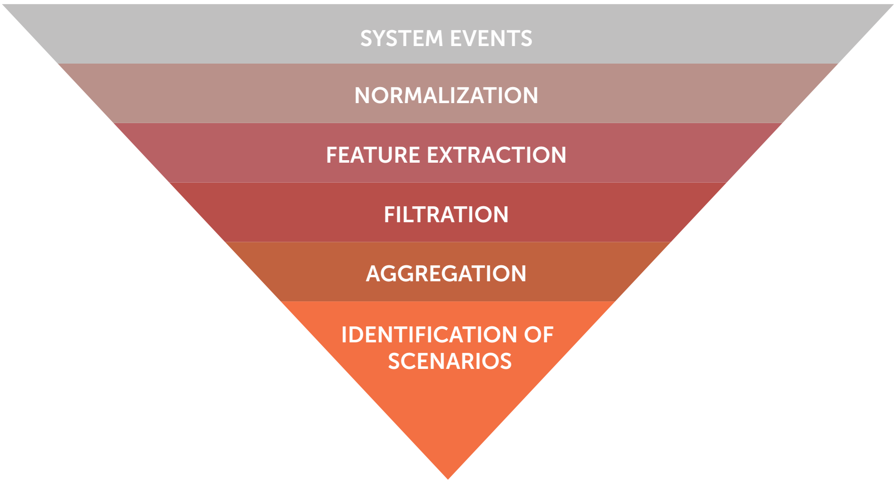
Another example is the prevention of exploits. In this case, malicious behavior is detected within a trusted application.

For example, when a Word document containing an exploit is opened, the Automatic Exploit Prevention (AEP) technology detects malicious behavior and blocks it. This technology is effective and can block complex threats, including exploits for 0-day vulnerabilities.

3.1 Behavior analysis

This technology analyzes the behavior of all active components within the trusted environment of the protected node. It consists of the following levels of analysis:

Behavior analysis



- system events – monitoring of essential system events, such as process creation, changes to the registry key values, modifications to files, etc.;
- normalization – arranging all incoming events into a common format for further processing;
- feature extraction – adding extra information for some events, e.g. whether a modified file is executable;
- filtration, aggregation, identification of scenarios – at these stages, significant combinations and sequences of events are identified, which add up to a behavior scenario. The library of malicious scenarios is created by Kaspersky Lab's automated center as a reference for threat processing and analysis.

3.2 Privilege control

Privilege control is executed in parallel with behavior analysis, based on application policies and categorization.

Control consists of monitoring application activities and enforcing restrictions based on an application's properties: popularity around the world, the publisher's trustworthiness, whether it triggers a detection, etc. Because of this, a program cannot perform uncontrolled actions within the protected environment, such as establishing network communications or other similar activities.

Basic restrictions for different categories of applications are generated by Kaspersky Lab's automated threat processing and analysis center.

For example, Microsoft applications or other well-known applications will be assigned a weak control policy. However, the privilege control system will assign little-known applications a correspondingly strict policy that matches the risks and level of danger that the application may pose.

Privilege control works in combination with Default Deny lists of trusted software programs (if enabled), thus ensuring security in real time. Restrictions can be managed centrally at the corporate network level, or, alternatively, protection of personal data can be configured on an individual basis.

4. Remediation after infection

An infection is the execution of malicious code within a trusted environment. In this case, the executed process works toward achieving the goals set by cybercriminals, generating a sequence of different events. Typically, such situations occur when the security solution is installed on a node that is known to be infected, or when potentially dangerous activity is detected at the behavior analysis level. An example would be when file encryption is launched by a legitimate process on the local drive of the protection node.

In 2016, 22.6% of users attacked by cryptors were from the corporate sector.

In such cases, the fourth stage of protection begins. This stage is responsible for the emergency response to a threat.

Every time behavior analysis technologies block a potentially dangerous activity, an action plan needs to be executed that reverts the trusted environment to its previous state.

4.1 Automatic rollback of actions

Automatic rollback of actions cancels any changes introduced, following the steps taken by the blocked process. It basically unravels the sequence of actions, reverting the structure to its previous state. It is aided by technologies from the **behavior analysis** stage that provide a detailed history of actions executed by each specific process.

A sequence of events may include:

- branches of the operating system registry;
- executable files created by the process (scripts or binary files);
- modified files, e.g. those that a cryptor has encrypted.

4.2 Advanced disinfection

In some complex cases (e.g. when a malicious code has injected itself into a system process that it is impossible to interfere with without affecting the stability of the operating system) the technology for treating an active infection gets involved. This tool is capable of securely restoring infected files, including components of the operating system. In the case of an active treatment, the protected computer is restarted. Infected system components are replaced with clean ones. When doing so, the technology relies on its ability to search for the original files required for restoration. The system is thus returned to a stable state.

In 2016, a total of 4,071,588 unique malicious and potentially dangerous programs were reported. (The number of unique programs is assumed to be the number of unique verdicts.)

4.3 Forensics

Analysis of each information security incident requires its own base of evidence. Because protection technologies collect a broad spectrum of data, an incident can be analyzed and preventive information security measures can be taken.

Inherent security measures

To ensure that the solution operates reliably, it has tools to control its own security. This ensures protection integrity, including protection from user attempts to disable it.

These self-defense tools intercept and block insecure operations with resources in the trusted environment, regardless of the user's rights and privileges. This resolves the issue of vulnerabilities that may allow a malicious program to gain administrator privileges.

Management

The Kaspersky Security Center component was developed for flexible security management. It provides detailed information about the status of endpoint security and about the centralized security policy. This makes Kaspersky Security Center the focal point for managing corporate network security as well as reports on all threats.

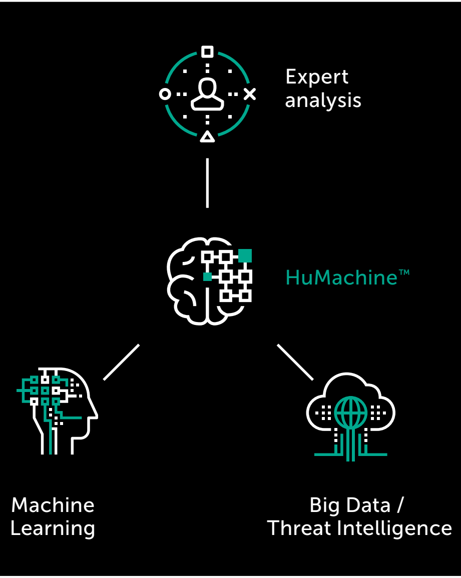
It is also important to mention the extended functionality available in Kaspersky Systems Management. It enhances the security of the corporate network thanks to the following features:

- vulnerability assessment and patch management;
- hardware and software inventories;
- flexible operating system and application provisioning;
- software distribution;
- SIEM integration;
- access control in complex corporate networks.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com


Expert analysis
HuMachine™
Machine Learning
Big Data / Threat Intelligence