KES 11 components and risk of their disabling

Protection components color description

🟥 Components that provide basic level of protection against threats. Not recommended to disable
🟨 Components that provide advanced protection
🟩 Components that provide additional protection features

Logic of the protection level indicator for the policy

Protection level	***Display conditions***
Low (red indicator)	***at least one red*** *component is disabled* ***OR*** ***at least two yellow*** *components are disabled*
Medium (yellow indicator)	***at least one yellow*** *component is disabled* ***AND*** ***all red*** *ingredients are enabled*
High (green indicator)	***all yellow*** *and* ***red*** *components are enabled* *(disabling any of the* ***green*** *components does not affect the color of the indicator)*

** According to the logic, a component is considered enabled if it is enabled in the product settings and the setting is protected from changes.*

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
File Threat Protection	*Essential Threat Protection*	File Threat Protection monitors the file system of the computer. It intercepts all file operations (such as reading, copying, executing) using a special driver and scans the files being accessed. If the file is infected, the operation is blocked, and the file is either disinfected or deleted if disinfection failed. File Threat Protection uses the following scanning technologies: signature analysis, heuristic analysis, and check against the cloud	• The computer has no access to the Internet, as well as any other resource (network, mail, IM, DVD, ...) **OR** • The ***Default Deny*** mode is enabled	Less than 50% of threats will be detected	• Malicious code can be executed	• Do not start new and unknown programs, do not open new and unknown documents • Use **Host Intrusion Prevention** to restrict activity of the mail clients, browsers, document viewers (e.g., Adobe Reader), download utilities, etc. • Use **Application Control** to configure the ***Default Deny*** mode

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Mail Threat Protection	*Essential Threat Protection*	Mail Threat Protection starts together with Kaspersky Endpoint Security, continuously remains active in memory, and scans all incoming and outgoing email messages on your computer for malware. It intercepts each email message that is received or sent by the user. If no threats are detected in the message, it becomes available to the user. Detection is based on signature and heuristic analyzers. The following protocols are supported: POP3, SMTP, IMAP, MAPI, and NNTP. Special plugins are provided for Microsoft Office Outlook and The Bat!	• E-mail is delivered via the corporate mail server with anti-virus and anti-spam solutions for mail servers installed (for example, KLMS) and running with recommended settings **OR** • **File Threat Protection** is enabled on the client and is running with recommended settings **OR** • Mail clients are not used on the client side		• Malicious content will be detected on the computer on later penetration stage • Malicious code can be executed	• Do not use mail clients • Do not open messages from unknown senders • Do not open attachments (including documents) from known senders • Do not open links in the messages • Use **Host Intrusion Prevention** to limit the activity of the mail clients • Use special products to protect mail servers from malicious and unwanted software, spam, and phishing links • Make sure **File Threat Protection** / **Web Threat Protection** / **Application Behavior Detection** are enabled and mail client is not in their exclusion list

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Web Threat Protection	*Essential Threat Protection*	Web Threat Protection intercepts all web traffic every time you go online and blocks scripts on websites if they pose a threat. All HTTP and HTTPS traffic is subject to careful inspection to detect and block malware in web pages along with phishing and suspicious sites. It uses signature analysis, heuristics, and cloud-based methods	• Web traffic passes through the corporate proxy server with an anti-virus for proxy server solution installed (for example, kav4proxy) and running with recommended settings. Note that in this case the following types of protection will be disabled: detection of malicious scripts during their execution, URL address filtering, protection from phishing, and some other protection types **OR** • Internet access is restricted by policies and only trusted web resources are allowed	Less than 90% of threats will be detected (up to 40% of threats are blocked by URL Filtering; additionally up to 11% of script threats are blocked during execution)	• Infected Web pages can be visited • Malicious code can be executed	• Do not use the Internet • Visit only trusted Internet resources • Use **Host Intrusion Prevention** to restrict browsers' activity • Use special products to protect proxy servers and Web gateways • Increase security level in the browsers' settings
Firewall	*Essential Threat Protection*	The Firewall component protects computer while it is connected to the Internet and other networks. It monitors inbound and outbound connections, ports, network packets and data streams. Firewall provides protection against network attacks of different kinds on network and application levels. Protection on the network level is provided by applying network packet rules. Protection on the application level is provided by applying rules according to which the installed applications can access network resources	Can be disabled in any configuration		• Unauthorized programs may access the network (which can result in important data leakage)	• Disconnect the computer from the network • Do not start new and unknown programs, do not open new and unknown documents • Use **Host Intrusion Prevention** to restrict activity of the mail clients, browsers, document viewers (like Adobe Reader), download utilities, etc. • Use **Application Control** to configure the ***Default Deny*** mode

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Network Threat Protection	*Essential Threat Protection*	Network Threat Protection scans inbound traffic for activity typical for network attacks like port scanning, denial-of-service, and other remote malicious actions. On detecting a network attack targeting your computer, Kaspersky Endpoint Security 11 blocks the network activity originating from the attacking computer. Network Threat Protection uses signatures and blocks all connections that match the descriptions of known network attacks	As a result of the component disablement, the computer may be vulnerable to certain types of network attacks, e.g. brute-force (password search), attacks using known vulnerabilities of network protocols (like WannaCry), DoS attacks etc. Even though using the component in the local network may reduce the system efficiency when accessing shared network resources, Kaspersky Lab strongly does not recommend to disable it. In general, component disablement significantly affects the system protection level and may cause an infection or data loss		• A network attack is possible that can result in executing malicious code or temporary computer break down	• Disconnect the computer from the network • Always install patches on all operating systems and applications as soon as possible, and use the latest versions of software

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
System Watcher*** ** In KES 11, the component has been divided into the following 3 components and is not present in the product interface* **Application Behavior Detection** **Exploit Prevention** **Remediation Engine**	*Advanced Threat Protection*	These 3 components monitor activity of all applications in the system. The information is analyzed using Behavior Stream Signatures and the applications that demonstrate malicious activity are blocked. Then the components roll back all the actions carried out by the application in the system (such as registry changes, hooks to Windows components, alteration of the hosts file, etc.) The rollback of malicious activity is performed automatically, depending on the policy settings, thus providing a complete solution for detection, prevention, and mitigation. These components also allow protecting the endpoint from malware that use vulnerabilities in popular applications, such as Abode Reader or Internet Explorer, to perform their harmful actions	• Disabling is possible, but if an unknown threat run, it cannot be detected by behavior **OR** • The ***Default Deny*** mode is enabled	Less than 94% of threats will be detected	• Vulnerabilities may be exploited when documents are opened • Malicious code can be executed	• Do not start new and unknown programs, do not open new and unknown documents • Use **Host Intrusion Prevention** to restrict activity of the mail clients, browsers, document viewers (like Adobe Reader), download utilities, etc. • Use **Application Control** to configure the ***Default Deny*** mode • Always install patches on all operating systems and applications as soon as possible, and use the latest versions of software

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Application Control	*Security Controls*	Application Control keeps track of all user attempts to start applications and regulates their launch using special rules with various conditions including path, metadata, hash, KL categories (a list of applications maintained by Kaspersky Lab specialists), and so on. The administrator can allow or block a user and/or group of users to start applications that match an Application Control rule. All user attempts to start applications are logged and can be found in reports	Control is not planned		- Start of unknown (potentially dangerous) or prohibited programs	- Use regular tools (for example, Active Directory policies) to prohibit the users from installing software, local administrator permissions, and other (UAC)
Host Intrusion Prevention	*Advanced Threat Protection*	Host Intrusion Prevention is actually an eponymous module ("HIPS") of the Kaspersky Endpoint Security. Its main purpose is to regulate the activities of the running applications like access to the file system and registry as well as interaction with other applications, and so on. It prevents applications from performing actions that may be dangerous for the system and ensures control of access to the operating system resources. Every application receives one of the four trust levels: trusted, low restricted, high restricted, or untrusted. Standard activity limits are pre-defined for each category. The administrator can change these restrictions within the categories. Additionally, individual limitations can be configured for every application in the policy	Additional setup is not planned		- Malicious code can be executed	- Do not start new and unknown programs, do not open new and unknown documents - Use **Application Control** to configure the ***Default Deny*** mode - Use regular tools (for example, Active Directory policies) to prohibit the users from installing software, local administrator permissions, and other (UAC)

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Device Control	*Security Controls*	Device Control ensures the security of endpoint and private data by restricting users' access to devices installed into the computer or connected to it. User access is managed by applying access rules based on the types of devices (hard drives, removable drives, Wi-Fi, Bluetooth, etc.), types of connection buses (USB, serial port, infrared, PCMCIA, etc.), and trusted devices (a list of removable drives in the company that must be allowed always and everywhere). It is possible to specify the access schedule and operation types. Kaspersky Endpoint Security also allows users to request temporary access to the blocked devices	Control is not planned		• Malicious code can be executed from external media • Leakage of important information via external media	• Physically restrict external media connections (USB, DVD, ...) • Use regular tools (for example, Active Directory policies) to prohibit the users from installing software
Web Control	*Security Controls*	Web Control provides control over users' access to web resources regardless of workstation location (inside or outside the corporate network). It is possible to block access, allow it, or show a warning. Web resources' access rules are actually sets of filters and actions that Kaspersky Endpoint Security performs when the user visits web resources described in the rules during the time span indicated in the rule schedule. Various and precise conditions can be used here including types of content, types of data, addresses, access schedule, and so on. HTTP and HTTPS protocols are supported	Control is not planned		• Malicious code can be executed when the users browse the Internet	• Do not use the Internet • Increase security level in the browsers' settings • Use **Application Control** to configure the ***Default Deny*** mode • Use **Host Intrusion Prevention** to restrict activity of browsers

KES 11 component	*Component category*	*Component brief description*	*Conditions of disabling*	*Detection rate loss on disabling the component (estimation)*	*Consequences of disabling*	*Actions on risk mitigation*
Kaspersky Security Network	*Advanced Threat Protection*	Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Endpoint Security to new threats, improves the performance of some protection components, and reduces the likelihood of false positives	The computer has no Internet access	Less than 94% of threats will be detected	• Malicious code can be executed • Risk of false positives is higher	• Increase update download frequency • Use **Application Control** to configure the ***Default Deny*** mode