# Kaspersky Next EDR Optimum

## Feature List

kaspersky

# Contents



# What is Kaspersky Next?

Kaspersky Next is your new security bedrock. Real-time protection, threat visibility, and investigation and response capabilities of EDR and XDR are delivered through progressive tiers, responding to your needs and available resources. This, together with cloud and on-prem deployment options, makes choosing your security easy, and growing your security quick and painless.

**Kaspersky Next**

### Kaspersky Next EDR Foundations

Recommended usage
IT team deals with security

Value
Ensure protection of all your endpoints

Key features:
- Endpoint protection
- Root cause analysis
- Security and IT management

### Kaspersky Next EDR Optimum

Recommended usage
Small cybersecurity team

Value
Boost your security with streamlined investigation and response

Key features:
- Advanced endpoint protection
- Cloud protection
- EDR guidance and automation

### Kaspersky Next XDR Expert

Recommended usage
Large cybersecurity team or SOC

Value
Main professional tool for your security experts

Key features:
- Full-feature EDR
- IRP workflow and alert aggregation
- ML and advanced detection

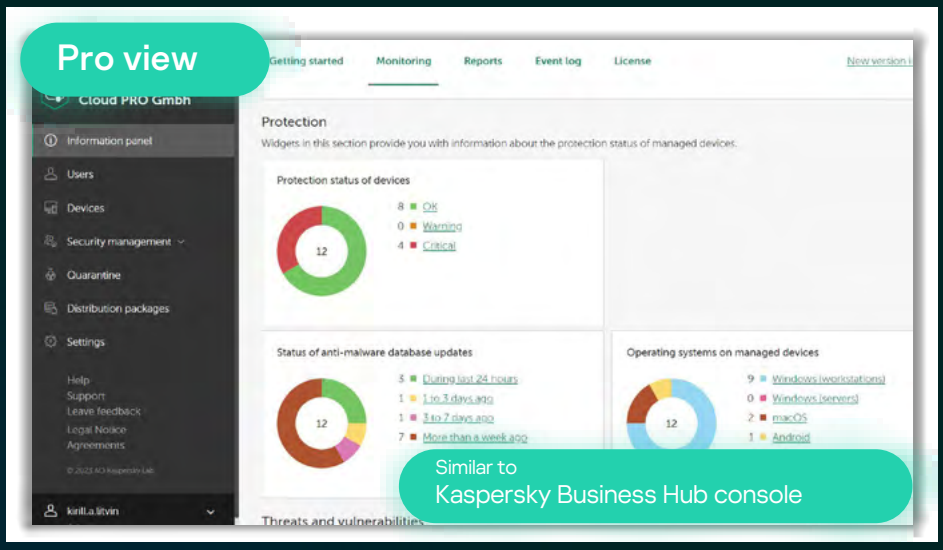
# What is Kaspersky Next EDR Optimum?

Kaspersky Next EDR Optimum provides strong endpoint protection, improved controls, training, patch management and more – all enhanced by essential EDR functionality. Threat visibility, investigation and response are simple, quick and guided to help you deflect attacks rapidly and with minimal resources.

# Features

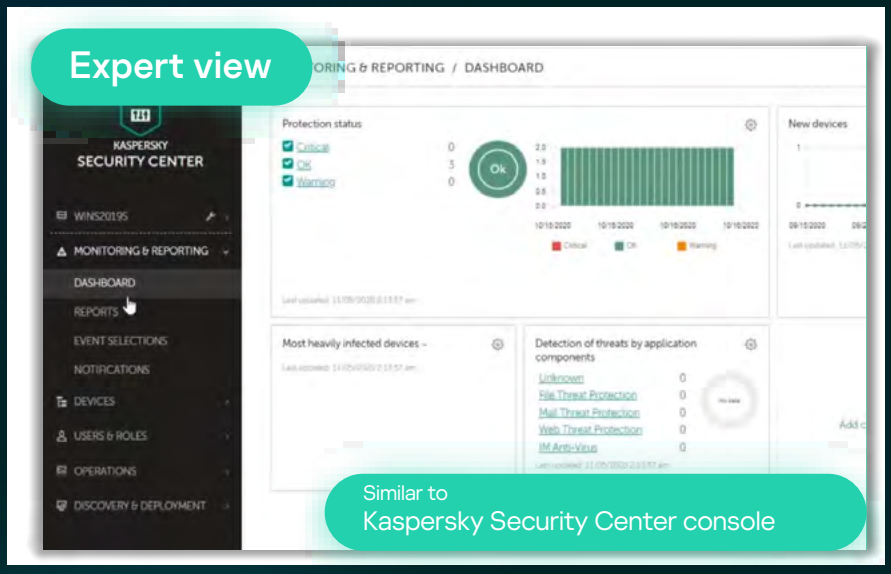
## A word about management consoles

Before we continue with the features, please keep in mind that Kaspersky Next EDR Optimum's management is available in several options:




**Pro view: Streamlined, easy to manage console hosted in the cloud.**

Maximum number of protected users: 2500




**Expert view: Customizable console with granular controls. Comes in three options:**

- Cloud based. Does not require hardware to install the management server or labor time to update it – it's all hosted and supported by Kaspersky.
- Minimum number of protected users: 300
- On premises, web console. Provides a web interface for creating and maintaining the protection system
- On premises, MMC. Implemented as a snap-in for Microsoft Management Console (MMC)

Please note: for on premises installations we highly recommend using the web console, as some features like EDR functionality might not be available in MMC.

# Endpoint protection

| Feature | Description |
|---|---|
| Multi-layered anti-malware | Our latest anti-malware engine combines signature-based protection, heuristic and behavioral analysis plus cloud-assisted technologies to protect your Windows workstations from known, unknown and advanced malware threats. Pattern-based detection technology improves detection rates and helps to reduce the size of update files, so you benefit from reliable security that consumes less of your communications bandwidth. |
| Behavior detection | Collects information about the actions of applications on a user's computer and provides this information to other components for more effective protection. |
| Exploit prevention | Tracks executable files run by vulnerable applications. When there's an attempt to run an executable file from a vulnerable application that wasn't initiated by the user, the component blocks the file from running. |
| Adaptive anomaly control | Monitors and blocks actions that are not typical of the computers in a company's network. Adaptive Anomaly Control uses a set of rules to track uncharacteristic behavior (for example, starting Microsoft PowerShell from an Office application. Rules are created by Kaspersky specialists based on typical malicious activity scenarios . |
| Remediation engine | Increases protection against cryptolockers by rolling back actions performed by malware in the operating system, including file, registry, system and network activity.<br>Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data. |
| File threat protection | Anti-virus detects and eliminates threats on a device in real-time by using the application's anti-virus databases and the Kaspersky Security Network cloud service. |
| Mail threat protection | This security application component scans incoming and outgoing email messages for threats. It starts when the application starts, resides in the device RAM, and scans all messages sent or received via the POP3, SMTP, IMAP and NNTP protocols. |
| Web threat protection | This component protects incoming and outgoing data that's sent to and from a device over HTTP, HTTPS and FTP protocols, and prevents dangerous scripts from running on the device. |
| Firewall | The firewall protects each endpoint against network threats when browsing the internet or using a local network. It blocks unauthorized network connections to the computer, reducing the risk of infection. It monitors the network activity of applications on the device, which reduces the risk of malware propagation in the network. It also restricts actions performed by users who violate the company's security policy (intentionally or otherwise). |
| Host Intrusion Prevention (HIPS) | Host Intrusion Prevention prevents applications from performing actions that may be harmful to the operating system, and controls access to operating system resources and personal data. |
| Network threat protection | This component scans a device's inbound network traffic for activity typical of a network attack, such as the intrusion of a remote device into the operating system. When Network Threat Protection detects an attempted network attack on the device, it blocks network activity from the attacking computer. |
| BadUSB Attack prevention | Prevents infected USB devices emulating a keyboard from connecting to the computer. When a USB device is connected to the computer and identified as a keyboard by the operating system, the application prompts the user to enter a numerical code generated by the application. This procedure is known as 'keyboard authorization'. |
| AMSI protection | Supports Antimalware Scan Interface (AMSI) from Microsoft. AMSI allows third-party applications that support it to send objects (for example, PowerShell scripts) to Kaspersky Endpoint Security for an additional scan and then receive the results from scanning these objects. |
| Kaspersky Security Network | Millions of consenting customers and thousands of businesses agree to allow the cloud-based Kaspersky Security Network (KSN) to receive anonymized data about malware and suspicious behavior from their computers. This real-time flow of data helps us deliver an extremely rapid response to new malware while also achieving a lower rate of 'false positives'. |
| Mobile threat defense | A set of protection capabilities to secure Android and iOS devices against viruses and other malware. See details by each OS type below. |

| Feature | Description |
|---|---|
| SIEM integration | Events can be exported to third-party SIEM solutions systems that deal with security issues on an organizational and technical level (i.e. SOCs). Supports Syslog and CEF/LEEF protocols. |
| EMM integration | Your existing EMM solution can be used to deploy and configure Kaspersky Endpoint Security for Android, aligning your security with current business processes. Supported third-party EMMs: VMware AirWatch, MobileIron, MS Intune, IBM MaaS360 and SOTI MobiControl. |

## Security management

| Feature | Description |
|---|---|
| **System hardening** | |
| Vulnerability assessment | Provides an overview of applications installed on corporate devices, and a list of available patches to update those applications to the latest versions. |
| Patch management | Lets you remotely manage application updates and patches on your corporate devices to ensure that you're using only the most up-to-date products. The list of applications is in the vulnerability assessment section of the product's online console. |
| Encryption management | Allows remote encryption of employee devices via the native Windows (BitLocker) and Mac OS (FileVault) encryption component to keep corporate data protected in case a device is lost or stolen. |
| Application control | Manages the startup of applications on users' computers and reduces the risk of computer infection by restricting access to applications. This allows you to implement a corporate security policy when using applications. |
| Web control | Allows control of user access to the internet depending on the site's content or location. Web URL blacklisting restricts users from accessing potentially harmful or undesirable websites. Whitelisting allows access to safe internet resources only. |
| Device control | Controls user access to external and removable devices connected to the computer. Administrators can allow or block the use of certain devices by type or create a 'trusted' list. |
| Remote wipe | Enables you to remotely delete data from users' computer. Protect data on a laptop in case it is lost or stolen. |
| Mobile Device Management (MDM) | Manage mobile devices owned by employees in your organization to apply corporate security requirements, control compliance, protect devices from threats and prevent leakage of corporate information. |
| **IT scenarios** | |
| Remote troubleshooting | By enabling secure, remote connections to a desktop or client computer helps you to resolve issues quickly and efficiently. An authorization mechanism prevents unauthorized remote access – and, for traceability and auditing, all activities performed during a remote access session are logged. Also includes remote diagnostics utility for troubleshooting of Kaspersky security applications on managed devices. |
| Installation of operating systems and applications | Kaspersky Security Center allows you to create operating system images and deploy them on client devices on the network, as well as perform remote installation of Kaspersky applications or those from other vendors. |
| Hardware and software inventory | Automated discovery and hardware and software tracking give administrators detailed insights into every asset on the corporate network. Automated software scanning enables rapid detection of outdated software that may pose a security risk if not kept up to date. |
| **Cybersecurity training** | |
| Cybersecurity training for IT specialists | This training will teach your IT administrators the basics of cybersecurity and help your security officer to detect and respond to threats.<br><br>The training is split into several modules, each comprising several sections. Each section begins with some theory, before learners move on to interactive assignments in a simulated Windows environment to learn first-level incident response skills. After completion of all sections within the module, learners can download a certificate of accomplishment. |

# Mobile threat protection

| Feature | Description | Pro view | Expert view |
|---|---|---|---|
| **Android** | | | |
| **Anti-virus protection** | Detects and neutralizes threats on your device by using anti-virus databases and the Kaspersky Security Network cloud service. Protects the device against threats, viruses, and other malicious applications in real time, scans new applications and distribution packages in the Downloads folder. Scans all files the user opens, modifies, moves, copies, runs and saves on the device. Blocks adware and applications that can be used by criminals to harm the user's device and data. | ✓ | ✓ |
| **Password protection** | Protects device access with a screen unlock password. | ✓ | ✓ |
| **Anti-theft** | Protects information stored on the device against unauthorized access if the device is lost or stolen. Remotely lock and locate the device, sound an alarm, or remotely wipe data from it. | ✓ | ✓ |
| **Application control** | Manage apps on users' devices using set of rules. You can configure two types of App Control rules: application rules and category rules. | ✓ | ✓ |
| **Compliance control** | Checks user device settings for compliance with corporate security requirements.<br>For example, if the device is rooted, and has outdated anti-virus databases – protective actions can be configured. | ✓ | ✓ |
| **Web control** | Blocks access to phishing and malicious websites. Monitors access to websites depending on their contents and location. | ✓ | ✓ |
| **Feature control** | Prohibit the use of device camera, Bluetooth and Wi-Fi modules on devices to minimize the risk of sensitive data leakage. Configure automatic connection to a corporate Wi-Fi network on Android. | ✓ | ✓ |
| **Wi-Fi configuration** | Defines Wi-Fi network settings when the device connects to the internet. | ✓ | ✓ |
| **Synchronization and databases update while roaming** | Run the device synchronization with the Administration Server while in the roaming area, and run anti-virus database updates while the device is roaming. Users can do both manually at any time. | ✓ | ✓ |
| **Root detection** | System files are unprotected on a hacked device and can be modified, and third-part apps from unknown sources can also be installed on hacked devices. When a root attempt is detected, we recommend that you immediately restore normal operation of the device. | ✓ | ✓ |
| **Mail configuration** | Set up Exchange mailbox to work with corporate mail, contacts, and the calendar on the mobile device | | ✓ |
| **KNOX/ Exchange ActiveSync (EAS) support** | Deployment of the Kaspersky Endpoint Security for Android app can be done through the Samsung KNOX Mobile Enrollment console. Exchange ActiveSync protocol can be used to configure restrictions of device features to keep an EAS device secure. | | ✓ |
| **Android Work Profile support** | Set up the separate container (by using Android Work Profile) for your corporate apps and data | | ✓ |
| **PKI integration** | Set up the connection to your MS CA and transfer the certificates for mail, VPN, Wi-Fi authentification to the connected mobile devices | | ✓ |
| **iOS** | | | |
| **Web control** | Monitors access to websites depending on their contents and location.<br>Settings are only applied to supervised devices. | ✓ | ✓ |
| **Web anti-phishing, anti-malware** | Secures iOS device from phishing and malware resources that employees may be facing. | | ✓ |
| **Password protection** | Protects device access with a screen unlock password. | ✓ | ✓ |

| Feature | Description | Pro view | Expert view |
|---|---|---|---|
| **Proxy settings** | Proxy Settings Protects traffic when connecting the device to the internet through a global HTTP proxy.<br>Settings are only applied to supervised devices. | ✓ | ✓ |
| **Anti-theft functionality** | Remote lock and wipe functions can be applied to a stolen device to protect against data loss. | ✓ | ✓ |
| **Feature control** | Restricts user access to the native iOS device features including camera control, apps installation, screenshots, AirDrop, iCloud, etc. In total, up to 40 various features are supported. Please note that some features can only be managed for supervised devices. | ✓ | ✓ |
| **Access Point Name configuration** | Configures Access Point Name (APN) when connecting to data services in a mobile network. | ✓ | ✓ |
| **AirPrint configuration** | Configures AirPrint for printing documents from the device | ✓ | ✓ |
| **Wi-Fi configuration** | Defines Wi-Fi network settings when the device connects to the internet | ✓ | ✓ |
| **Email setup** | Configures email accounts belonging to the device user. | ✓ | ✓ |
| **CalDAV setup** | Configures CalDAV accounts belonging to the device user for handling the calendar. | ✓ | ✓ |
| **Calendar subscriptions** | Configures subscription to third-party calendars for adding events to the device. | ✓ | ✓ |
| **Jailbreak detection** | System files are unprotected on a hacked device and can be modified. When a jailbreak is detected, we recommend that you immediately restore normal operation of the device. | | ✓ |

## Cloud security

| Feature | Description |
|---|---|
| **Cloud Discovery** | Enables the discovery and restriction of inappropriate or unauthorized cloud resources usage, as well as the time wasted on social networks and messengers. Monitor 2700+ cloud services.<br>Every detected cloud service now has a rating that indicates how dangerous use of the service is. This means that IT admin can easily assess potential risks and decide to allow or block a particular service. |
| **Cloud blocking** | Block user access to inappropriate or unauthorized cloud resources, social networks or messengers. |
| **Data Discovery** | It provides visibility and control on the data stored in the cloud to prevent data loss and meet compliance standards. Data discovery gain visibility and control of sensitive data in MS Exchange Online, SharePoint Online, OneDrive and Teams. Detect results can be found in reports and the detection list, as well as on the dashboard widgets. Audited file types: doc, docx, ppt, pptx, xls, xlsx, odt, odp, ods, PDF, RTF, jpeg, tiff, png, jp2.<br>• Credit/Debit card number<br>• Brazilian: Driver License, Identity Card (RG), Individual Taxpayer Registry (CPF), Passport<br>• Colombian: Driver License, Identity Card, Passport, Unique Taxpayer Number (NIT)<br>• French: Driver License, Identity Card, Passport, Social Security Number<br>• German: Driver License, Identity Card, Passport, Residence Permit, Social Insurance Number (SIN), Tax Identification Number (TIN)<br>• Italian: Driver License, Identity Card, Passport, Fiscal Code<br>• Mexican: Citizen Card (CURP), Individual Taxpayer Registry (RFC), Passport, Social Security Number<br>• Portuguese: Driver License, Citizen Card, Passport, Social Security Number (NISS), Tax Identification Number (NIF)<br>• Spanish: Identity Card, Passport. National Insurance Number, Unique Taxpayer Reference<br>• UK: Driving License, Passport, Residence Card, National Insurance Number, Tax Identification Number (TIN)<br>• US: Driver License, Passport, Social Security Number (SSN), Individual Taxpayer Identification Number (ITIN) |

| Feature | Description |
|---|---|
| Security for Microsoft Office 365 | Advanced threat protection - anti-phishing, anti-malware, anti-spam, removal of unwanted attachments and protection on demand - for all major MS Office 365 applications. For more details please check out Kaspersky Security for Microsoft Office 365 |

# Essential EDR capabilities

| Feature | Description |
|---|---|
| **Visibility & Investigation** | |
| Alert card with root cause analysis | **Alert card overview**<br>Each new detect is opened and populated with automatically generated information after malicious/suspicious activity has been detected on the endpoint. The alert card is generated by the management console and includes, among other things, the following categories of information:<br>• Drill-down threat propagation graph<br>• Alert events (registered artifacts - file/process details, URL information, registry modifications, etc.)<br>• Host information (name, IP address, MAC address, list of users, OS domain controller role, etc.)<br>• General information on detections, including detection mode (ODS/OAS/AMSI/on execute, etc.)<br>• Registry changes, autorun detects<br>• Response status (i.e. quarantined, disinfected)<br>• Data on the file, including name and path, MD5/SHA256 hash, appearance history, etc.<br>Most investigation and response actions are performed in this alert card.<br>**Root cause analysis overview**<br>This section at the top of the alert card includes the threat propagation graph which contains key processes, network connections, DLLs, registry hives affected or involved in the alert.<br>All detections are highlighted on the graph, providing the analyst with full context of the incident and facilitating the process of revealing affected components.<br>The graph provides drill-down capabilities with additional information on processes, etc.<br>All gathered alert-related data can be sorted by group (processes, registry, connections, etc.) or by list. |
| Threat Intelligence information | A file's reputation from our Kaspersky Threat Intelligence Portal is integrated into the alert card for even faster and more accurate root cause analysis. Available data includes:<br>• Status in Kaspersky Security Network<br>• Number of KSN users encountering this file<br>• Geography of KSN users encountering this file<br>• Date of first appearance<br>For more information on the detected file, the user can follow the built-in link to the Kaspersky Threat Intelligence Portal (paid or free version). |
| **Indicators of Compromise (IoCs)[1]** | |
| Reactive approach | Threat indicators (IoCs) for a specific alert, or a file found in the threat propagation graph, can be automatically generated and an IoC scan can be launched based on this IoC.<br>The list of indicators is generated based on the data gathered for the associated alert and presented to the security officer for further actions, such as search for a similar incident on other hosts or automatic cross-endpoint response.<br>The list of IoCs can be found in the alert card.<br>Search for similar incidents by scanning the infrastructure using IoCs automatically generated by the system. The indicators can be preselected by the user before the scanning process occurs.<br>If multiple IoCs are used, the user can set up logic rules for detection.<br>The user can also set up automated response actions when running IoC scans (see Response section below). |

| Feature | Description |
|---|---|
| **Proactive approach** | To simplify the work of security officers in identifying IoCs, third-party IoCs in OpenIOC format can be uploaded to the system (e.g. from any threat intelligence provider, regulation body or other source, such as securelist.com).<br><br>Search is carried out using file-based threat indicators (file hashes). The list of supported OpenIOC terms can be shared by Kaspersky. Validity checks of IoC terms are performed to ensure IoC syntax correctness and full support when importing the file/list of files..<br><br>**Please note:** in Pro view adding IoC is possible by inserting a copied file hash into a simple text box. Expert view requires creating or modifying an existing openIOC file (XML format). |
| **IoC scan: scheduled scan** | IoC scanning of endpoint infrastructure can be carried out according to a schedule. The scanning process takes place directly on the endpoints, and their current status is checked. |
| **IoC export** | Automatically generated artifacts related to the alert can be exported and saved in OpenIOC format. |
| **Response** | |
| **Response guidance** | The alert card contains a section for response recommendations. Suggested actions are listed as step-by-step instructions with clickable links that show where certain actions can be performed.<br><br>This allows the user to quickly learn how to use the solution and have guidance in case of an urgent, fast-moving threat. |
| **'Single-click' response** | Rapid response actions cut response times from hours to minutes and reduce the number of routine manual tasks through a wide range of automated response actions.<br><br>Most response actions are available in the alert card or in the threat propagation graph drill-down and can be performed in just a few clicks.<br><br>In the alert card several response actions are available as separate buttons:<br><br>• Execution prevention<br>The object is added to the blocklist. The task can be performed over the entire endpoint infrastructure.<br>• Host isolation<br>The current host or remote host can be isolated from the rest of the network to prevent further spread of the threat.<br>In this case, connection to the management console is preserved.<br>Custom host isolation exclusion rules can be configured (i.e. by adding particular network resources to exclusions, e.g. DNS or selecting predefined profiles).<br>• Quarantine file<br>Moving an object to the special repository for storing suspicious objects. Quarantined files are stored on the protected device in an encrypted form and therefore do not compromise the device security. Available in Expert view. |
| **Console response** | Some response actions are available from outside the alert card, including but not limited to:<br><br>• Add to allowlist<br>Allowlisting the object using Endpoint Protection and System Management functionality from the management console.<br>• Get file<br>Allows the security officer to get files from user devices. For example, you can configure getting an event log file created by a third-party application. As a result of the execution of the task, the file is saved in Quarantine. You can download this file from Quarantine to your device using the management console. On the user device, the file remains in its original folder.<br>• Delete file<br>Objects can be remotely deleted from a single endpoint or a group of hosts.<br>• Start process<br>Any additional software can be run remotely on the host.<br>• Terminate process<br>Stopping execution of suspicious processes - any process can be remotely killed on an endpoint. to contain the threat on the endpoint and to block data exfiltration and lateral movement attempts in real time. |

[1] Indicators of Compromise are traces of malicious activity, such as hashes of malicious files, which when found on a target endpoint, can indicate that it's been infected or is currently under attack.

| Feature | Description |
|---|---|
| **Automatic cross-endpoint response with IoC scan** | Threat indicators (IoC) for a specific alert or file found in the threat propagation graph can be automatically generated and an IoC scan can be launched based on this IoC.<br>These response actions include:<br>• Host isolation<br>See above<br>• Critical areas scan<br>Scanning the critical areas using Endpoint Protection functionality. Available only during IoC scan.<br>• Quarantine copy and Delete file<br>See above |
| **System critical object check** | If certain response actions, such as Terminate process or Delete file, are launched against a legitimate object critical to system operation, this action will be blocked as to not hinder normal system operation.<br>This setting can be changed in the Prevention rules group of settings. |
| Recovery | |
| **Recover file from quarantine** | Any object stored in Quarantine can be recovered back to the endpoint at any time |
| **Remove network isolation** | Isolated hosts can be enabled on the network by the security officer. The time out value for isolation rules can be configured.<br>For example, this action can be performed with a button in the alert card, once the investigation and response are finished. |

# Supported devices and operating systems

What the icons in the table below mean:

available on Windows — System requirements

available on MacOS — System requirements

available on Linux — System requirements

available on iOS — System requirements

available on Android — System requirements

| Feature | Pro view | Expert view cloud | Expert view on-prem |
|---|---|---|---|
| **Endpoint protection** | | | |
| Behavior detection | ✓ | ✓ ✓ | ✓ ✓ |
| Exploit prevention | ✓ | ✓ | ✓ |
| Adaptive anomaly control* | ✓ | ✓ | ✓ |
| Remediation engine | ✓ | ✓ | ✓ |
| File threat protection | ✓ ✓ | ✓ ✓ ✓ | ✓ ✓ ✓ |
| Mail threat protection | ✓ | ✓ | ✓ |
| Web threat protection | ✓ ✓ | ✓ ✓ ✓ | ✓ ✓ ✓ |
| Firewall | ✓ | ✓ ✓ | ✓ ✓ |
| Host Intrusion Prevention (HIPS)* | ✓ | ✓ | ✓ |
| Network threat protection | ✓ | ✓ | ✓ |
| BadUSB Attack prevention | ✓ | ✓ | ✓ |
| AMSI protection | ✓ | ✓ | ✓ |
| Kaspersky Security Network | ✓ ✓ ✓ | ✓ ✓ ✓ ✓ | ✓ ✓ ✓ ✓ |
| Mobile threat defense | ✓ ✓ | ✓ ✓ | ✓ ✓ |
| SIEM integration | | ✓ | ✓ |
| EMM integration | ✓ | ✓ | ✓ |

| Feature | Pro view | Expert view cloud | Expert view on-prem |
|---|---|---|---|
| **System hardening** | | | |
| Vulnerability assessment | | | |
| Patch management | | | |
| Encryption management | | | |
| Application control | | | |
| Web control | | | |
| Device control | | | |
| Remote wipe | | | |
| Mobile Device Management (MDM) | | | iOS MDM: only in MMC |
| Remote troubleshooting | | | |
| Installation of operating systems and applications | | | |
| Hardware and software inventory | | | Linux: software inventory only |
| **Cybersecurity training** | | | |
| Cybersecurity training for IT specialists | ✓ | ✓** | ✓** |
| **Cloud security** | | | |
| Cloud discovery | ✓ | ✓ | ✓** |
| Cloud blocking | ✓ | ✓ | ✓** |
| Data discovery | ✓ | ✓** | ✓** |
| Security for Microsoft Office 365 | ✓ | ✓** | ✓** |
| **Essential EDR: Visibility & Investigation** | | | |
| Alert card with root cause analysis | | | |
| Threat Intelligence information | | | |
| **Essential EDR: Indicators of Compromise (IoCs)** | | | |
| Reactive approach | | | |
| Proactive approach | | | |
| IoC scan: scheduled scan | | | |
| IoC export | | | |

* not available for servers

** if you are using Expert view in cloud, you can create a Pro view account and use this functionality there

| Feature | Pro view | Expert view cloud | Expert view on-prem |
|---|---|---|---|
| **Essential EDR: Response** | | | |
| Response options | ✓ | ✓ | ✓ |
| Response guidance | ✓ | ✓ | ✓ |
| 'Single-click' response | ✓ | ✓ | ✓ |
| Console response | | ✓ | ✓ |
| Automatic cross-endpoint response with IoC scan | ✓ | ✓ | ✓ |
| System critical object check | | ✓ | ✓ |
| **Essential EDR: Recovery** | | | |
| Recover file from quarantine | ✓ | ✓ | ✓ |
| Remove network isolation | ✓ | ✓ | ✓ |

# Multitenancy

Multitenancy is an operation mode when the solution is used to protect the infrastructure of several organizations at the same time.

This mode has the following advantages:

- Makes it easy for MS(S)Ps to look after the security needs of multiple customers, remotely and without added complexity
- Simplifies security management for businesses with geographically distributed offices
- Copy security profile settings within workspaces – to minimize configuration time

Kaspersky Next EDR Optimum multi-tenancy allows MS(S)Ps[1] to offer EDR and endpoint protection as a service. Kaspersky Next EDR Optimum has full-fledged tenants, which means that there is data differentiation, i.e. users of one tenant cannot see the data (events, alerts, users, etc.) of other tenants. At the same time, the main administrator (the MS(S)P) has access to their subordinate tenants, and can build detection and response processes for their customers.

Key MS(S)P-ready capabilities include:

- Multiple administrators
  The solution can be managed together with the end-customer, if required
- Multiple workspaces
  See several workspaces in a single console window to manage multiple organizations
- Co-management
  MS(S)Ps can connect external admins or client admins for co-management
- Reporting
  Send customized reports on schedule
- Flexible monthly billing
  Change the number of protected nodes, connect new customers, and pay for the maximum number supported in that month
- Integration with popular Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) tools

[1] MSP – Managed Service Provider, MSSP – Managed Security Service Provider

Find out more about Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations — Learn more

Kaspersky Next XDR Expert — Learn more

Learn more about Kaspersky Next at:
https://go.kaspersky.com/next

Choose the tier that suits you best by taking a short survey in our interactive tool:
https://go.kaspersky.com/Kaspersky_Next_Tool

Cyber Threats News: securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

**kaspersky.com**