Feature list

Kaspersky Next EDR Expert

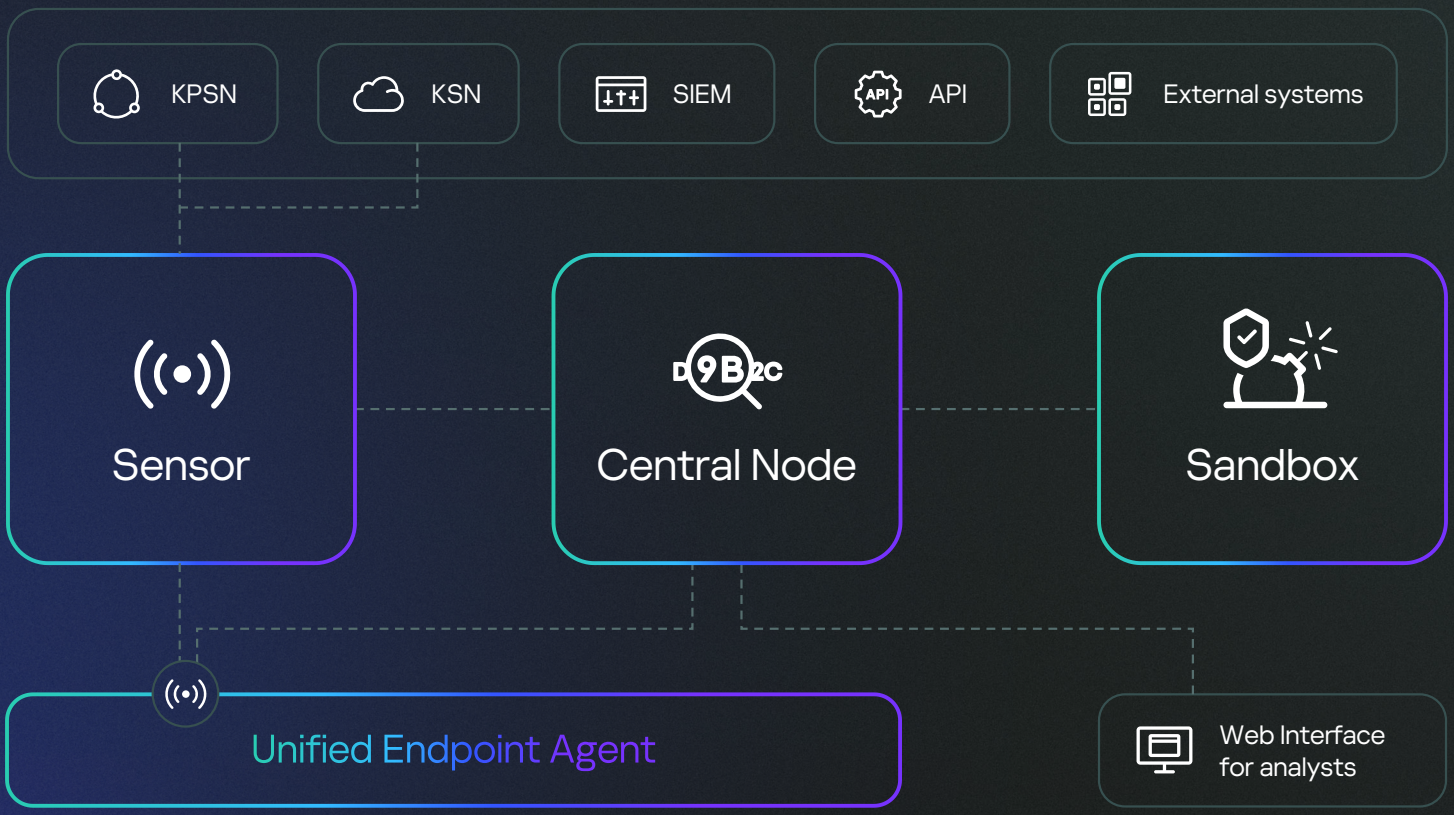
kaspersky bring on the future

Kaspersky Next EDR Expert

Solution overview

Kaspersky Next EDR Expert is a powerful Endpoint Detection and Response solution that works together with endpoint protection (EPP) to block mass attacks. It also provides effective advanced detection of complex threats, supports the investigation process powered by Kaspersky Threat Intelligence and the MITRE ATT&CK knowledge base, and delivers proactive threat hunting with a centralized response to multi-staged complex attacks targeting endpoint infrastructures.

Solution architecture



Sensor

Receives data from hosts protected by the endpoint agent or Kaspersky Endpoint Security and transmits it to the server with the Central Node component.

Central Node

The main server component of the platform, it performs data verification and analysis and publishes research results in the platform's web interface.

Sandbox

Runs virtual images of operating systems and monitors file behavior to detect malicious activity and signs of targeted attacks on the organization's IT infrastructure.

Key benefits

Unique technology stack

- Proprietary anti-malware engine
- Advanced sandbox
- Global reputation database (KSN)
- Integration with Threat Lookup
- Targeted Attack Analyzer (1500+ IoA rules)
- Mapping to MITRE ATT&CK

Automated and manual response scenarios

- Creation of automatic rules to block file execution based on sandbox verdicts
- Sending objects to sandbox manually or using API
- Recommendations for guided response
- Automated response scenarios in EPP

Global recognition

- High ratings from international agencies
- Supports regulatory compliance
- Trusted by major clients worldwide

Main elements and feature highlights

Endpoint agents

Endpoint agents gather all the necessary data from endpoints across the infrastructure (PCs, laptops, servers and VMs). The solution uses an integrated EPP agent for Windows, Linux and MacOS operating systems.

Agents deployed on endpoint operating systems constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They send the collected data and information related to the detection of suspicious events to Kaspersky Next EDR Expert for additional study and analysis, as well as for comparison with events detected in other information flows.

Examples of data transferred by our EDR agent to the server:

1. Start / end process
2. DLL loading
3. Remote host connection
4. Sending an HTTP request
5. Block a starting process
6. File creation
7. Events from the Windows event log
8. Kaspersky Endpoint Security (KES) detects and automatic response results, etc.

Centralized data and verdict repository

Metadata accumulated in the database is centrally stored, allowing the IT security team to conduct retrospective analysis and assist response services and regulatory authorities when required, providing them with the necessary information about detected threats and related events. The database also accumulates objects and verdicts received from detection mechanisms and the sandbox, so that data can be correlated with real-time events and new verdicts. All this enables more effective investigation of long-term multi-stage attacks.

Data storage for on-premise delivery is scalable and includes customizable data retention (data is retained for 30 days by default). Telemetry in the case of cloud delivery is retained for 30 days by default. The retention period can be extended to 60 or 90 days depending on the licensed option. Alerts/incidents in the case of cloud delivery are retained for 360 days.

Advanced detection mechanisms

Complex threats and extended attacks using unknown malicious code, compromised accounts, fileless methods, legitimate applications and unsuspected actions require a multi-level approach to detection with advanced technologies.

Sandbox

The sandbox runs suspicious objects on its own virtual machines to detect malicious activity. The sandbox receives sample execution tasks which include virtualization parameters based on the source of the evaluated object and the purpose of the evaluation (e.g. type of OS(s), OS configuration, environment, parameters of sample start, execution duration).

The sandbox can be used with the following OSs: Windows XP, Windows 7, Windows 8.1, Windows 10, CentOS 7.8 and Astra Linux 1.7.

During sample execution, the sandbox collects:

- Logs of the sample's behavior (including a list of system functions calls, iteration with other processes and files, network activities, URLs, etc.)
- Dumps
- Dropped objects
- Traffic generated by the sample

Settings of the Windows OS in the sandbox images can be configured to better fit your environment. These settings include:

1. Installed applications
2. Computer name
3. User account name
4. System language: Russian, English, Chinese, Arabic, Mexican Spanish

Once execution is complete, the artefacts acquired are stored, then processed by a dedicated scanner. If the sample proves to be malicious, a verdict is attributed, and the suspicious activities occurring during analysis in the sandbox are mapped to the MITRE ATT&CK knowledge base. All the collected data is stored internally to enable further analysis of the adversary's tactics and techniques without the need for additional sandbox requests, saving on server resources.

A comprehensive set of features, including OS environment randomization, time acceleration in virtual machines, anti-evasion techniques, user activity simulation, etc., contribute to highly efficient behavior-based detection. The sandbox uses various patented technologies and can be operated in automated and manual mode.

Kaspersky Security Network (KSN) / Kaspersky Private Security Network (KPSN)

Kaspersky Security Network (KSN) is a global cloud infrastructure that holds reputation verdicts and other information about objects processed by Kaspersky Next EDR Expert (files, domains, URLs, IP addresses and more). KSN also provides detection using cloud ML models, such as Cloud ML for Android - local APK file metadata is collected by Kaspersky Next EDR Expert and sent to KSN, which responds with a verdict created by the ML-based model.

For organizations with strict privacy policies, such as financial services or government agencies, Kaspersky Next EDR Expert can work in a completely isolated mode, without transferring any data outside the organization's perimeter. This is achieved through the Kaspersky Private Security Network (KPSN), and enables the customer to receive locally all the advantages of Kaspersky's global cloud reputation database (KSN). In addition to private access to our global threat intelligence database, verdicts from EDR Expert are stored on a local KPSN database and automatically shared with other Kaspersky products deployed within the organizational infrastructure for automated response. Organizations with KPSN deployed benefit from reputations provided by external third-party systems with no intermediate steps, via an API.

IoA engine

The IoA engine detects suspicious actions using a unique set of Indicators of Attack (IoAs) generated by Kaspersky's threat hunters, enabling real-time automated threat hunting. It supports automatic analysis of events and correlation with this unique set of IoAs. Every time a significant suspicious event is detected by the IoA engine, the IT security specialist receives a written description, recommendations (such as how to reduce the risk of a recurrence of the discovered event), and an indication of the confidence in the verdict and severity of the event to help in ranking. IoAs are mapped to MITRE ATT&CK to provide detailed information including the ATT&CK-defined technique used, a description and mitigation strategies. This means users automatically benefit from top-level threat research without overloading in-house experts, freeing up their time for other complex tasks like deep incident investigation and proactive threat hunting. IT security experts can also create their own database of custom IoAs appropriate to their particular infrastructure, for example, or to their industry sector.

Response toolset

Kaspersky Next EDR Expert provides automated, semi-automated and guided response capabilities.

Automated response

1

Kaspersky Next EDR Expert with included endpoint protection component (KES) enables automated response capabilities for most detected threats without having to involve IT security specialists. The Remediation Engine in KES rolls back actions that have been performed by malware in the operating system.

2

Kaspersky Next EDR Expert also allows the creation of auto prevention rules based on sandbox network detects.

Semi-automated response

IT security experts are equipped with tools that enable 'one click' responses from the central management console, reducing the number of routine manual tasks undertaken, and cutting response times from hours to minutes. A wide range of response activities are supported, including:

- Kill processes
- Quarantine / recovery of objects
- File deletion
- File transfer to the sandbox for analysis
- Running specific scripts or third-party programs on a dedicated endpoint
- Performing full host isolation
- Putting objects in prevention mode

Guided responses

Recommendations are categorized under four types of action:

Qualifying — depending on the type of alert, may include:

- Lookup in Kaspersky Threat Intelligence Portal by hash
- Show sandbox report
- Find related alerts by host name, URL or IoC
- Find KES event

Containment — depending on the type of alert, may include:

- Host isolation
- Create a prevention rule
- Create task

Investigation — depending on the type of alert, may include:

- Find related events
- Save alert indicators as IoA

Close — depending on the type, may include:

- Restore from quarantine
- Disable host isolation
- Delete prevention rule

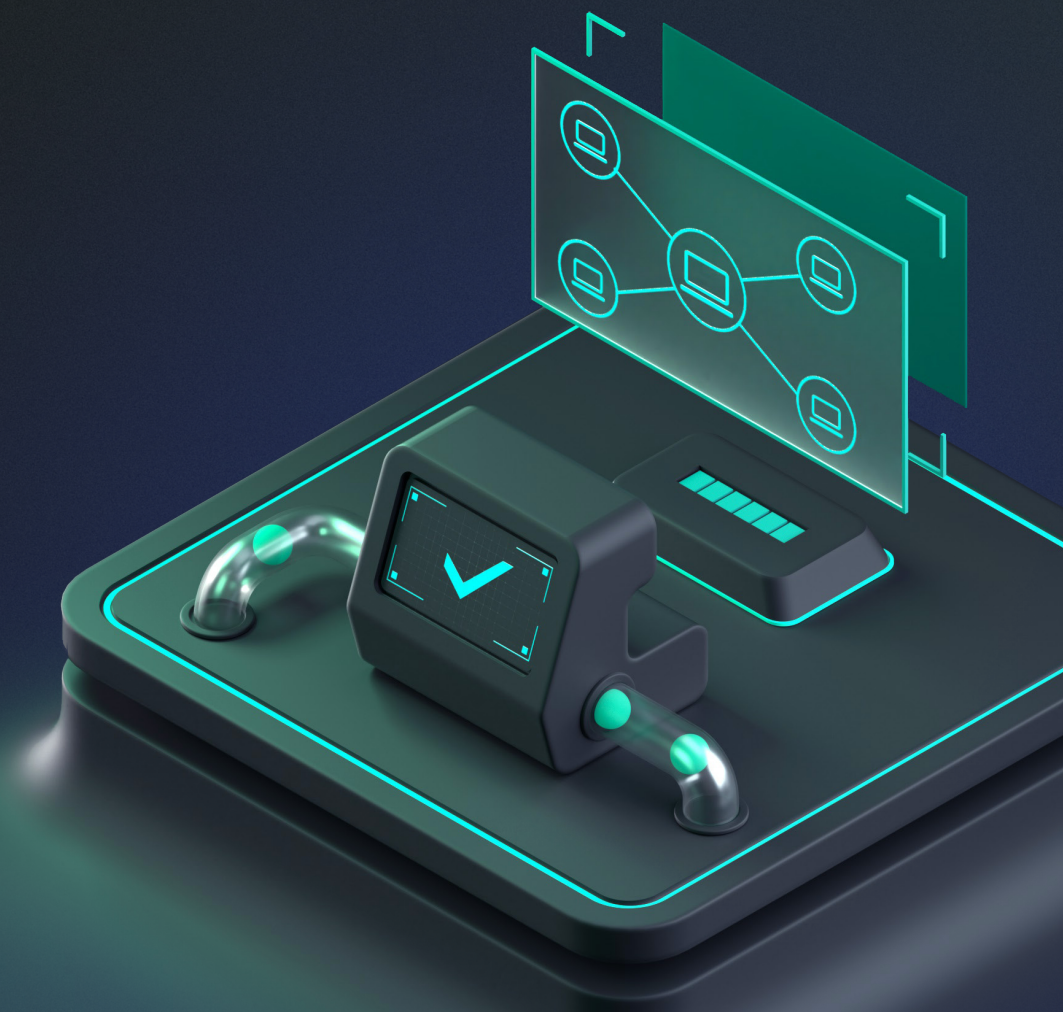
Single web console

The single web console is a convenient tool for monitoring alerts, centralized management, visualizing progress through the various threat search stages, studying the results of analysis, and monitoring the response process. Connection to the web interface is via any popular web browser. Access rights are issued in accordance with predefined roles (RBAC support).

Kaspersky Next EDR Expert supports failover cluster in active-active mode. The Central Node component can be deployed as a fault-tolerant cluster that has two roles: storage servers and processing servers. A cluster can consist of physical or virtual servers.

Integration

Full integration with Kaspersky Private Security Network. SIEM/SOC integration is available via Syslog (CEF is supported).



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 shares this information with 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.
Remediation engine	Increases protection against cryptolockers by rolling back actions performed by malware in the operating system, including file, registry, system and network activity. 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.
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 type of OS below.
SIEM integration	Events can be exported to third-party SIEM solutions 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.

Detection

1 Automated detection

Feature	Description
Enhanced anti-malware engine	Working on a Central Node, with more stringent settings than are enabled on endpoint configurations, the engine scans objects for malicious or potentially dangerous code and sends such objects to the sandbox. This results in highly accurate detections that can be of significant value during incident investigation.
Detection with YARA rules	YARA is one of the most widely used tools for hunting new variants of malware. It supports complex matching rules to search files with specific characteristics and metadata — for example, strings that characterize a particular coder's style. It's possible to create and upload customized YARA rules in order to analyze objects for threats specific to the organization. New scan areas are available for scanning with YARA rules on endpoints: • RAM • Specified folders • All local disks • Autorun points Kaspersky APT Intelligence Reporting provides a detailed technical description of the APT, including the related YARA rules description, giving security specialists and APT analysts actionable recommendations for optimum protection against the related threat.
Certificate verification	The Certcheck module checks for the presence of suspicious certificates as well as the validity of signed certificates.
Automatic event matching with data from cloud-based threat intelligence	Automated real-time access to Kaspersky Security Network (KSN) allows you to conduct reputation scans of objects and files. The continuous automated exchange of information about the reputations of files, Internet resources and software enables a faster response to the latest threats.
Automatic event matching with data from on-premise threat intelligence	Kaspersky Next EDR Expert supports the local version of KSN — Kaspersky Private Security Network (KPSN) — designed for organizations unable, for reasons of policy or regulatory compliance, to release or transfer any data outside their perimeter. KPSN detect attacks locally, without relying on a cloud service and with no reduction in detection levels.
Cloud ML for Android	Local APK file metadata is collected by Kaspersky Next EDR Expert and sent to KSN, which - using the advanced cloud-based ML-APK analysis engine — replies with a verdict created by the ML-based model.
Machine learning techniques	Kaspersky Next EDR Expert uses machine learning techniques for advanced analysis of endpoint behavior and APK files, and for object emulation.
Automatic integrated analysis of suspicious processes / files by sandbox	Provides the opportunity to investigate in detail the behavior of analyzed objects after they're placed in an isolated environment, and to use the information obtained when investigating complex incidents. Sandbox features include: • Auto submission of files from endpoints • Multi-level assessment and behavior analysis of emulated objects • Built-in specialized network interface for monitoring interactions of malicious objects with Internet resources • Simulates the actions of ordinary users • Effectively counteracts modern sandbox bypass techniques used by malware • Several emulation modes are supported
Analysis of password-protected archives and documents	Password checking mode supports password-protected archives and Office documents in PDF, MS Word, Excel and PowerPoint.

2 Semi-automated detection

IoC-based detection

EDR Expert allows centralized IoC loading from threat data sources and supports automatically scheduled IoC scanning, streamlining analysts' work. Retrospective database scans enrich the quality of information about previously flagged security events and alerts.

Check endpoint infrastructure for Indicators of Compromise (IoCs)	To help information security specialists identify Indicators of Compromise more efficiently, EDR Expert can upload IoCs in OpenIoC format, and configure automatic IoC verification scripts.
IoC scan queries over endpoints	IoC scanning of endpoint infrastructure can be scheduled. The scanning process takes place directly on endpoints, and checks their status.
Centralized scanning of retrospective data variants	Centralized IoC scanning of retrospective databases can be checked on-demand.

IoC scan reporting alerts

Reporting alerts include detailed information on which IoCs were detected, on which hosts, and on which rule branches.

IoA-based detection

EDR Expert with an IoA engine detects suspicious actions using a unique set of Indicators of Attack (IoAs) generated by Kaspersky's threat hunters, enabling real-time automated threat hunting.

Event correlation with Kaspersky unique IoAs	When processing telemetry from endpoints, automatic analysis of all events is supported, together with correlation to a unique set of Indicators of Attack (IoAs) obtained from Kaspersky's internal database generated by Kaspersky's threat hunting team. Matched IoAs in the user interface provide clear event descriptions, examples and counteraction recommendations.
Event chain-based threat detection	Events are analyzed not as isolated attack indicators, but as interconnected elements of activities characteristic of cyberattacks.
Ability to create a custom IoA database	All new events are automatically mapped in real time to an internal database of custom IoAs, enabling the immediate creation of informed response actions and long-term detection scenarios according to the specifics of the protected infrastructure.
Sigma rules support	The system allows the creation of a TAA (IoA) rule based on event search conditions from a YAML file with a Sigma rule.
IoA exclusions	Predefined IoAs can be excluded or granular exclusions can be applied to specific IoA rules.
Root cause analysis	All actions on hosts are centrally displayed in the interface facilitating effective root cause analysis. This gives analysts a complete view of an attack, helping them to quickly find the information they need for a response.

Retrospective analysis	Automated data, object and verdict collection, along with centralized storage enables retrospective analysis during multi-stage investigations – even when compromised endpoints are inaccessible or when data has been encrypted by cybercriminals.
Mapping to the MITRE ATT&CK framework	IoAs and sandbox detections are mapped to MITRE ATT&CK to support the analysis of adversary tactics, techniques, and procedures. Individual events in the incident tree are enriched with MITRE ATT&CK context, including identified tactics used and a visual representation of the event on the incident graph. IT security specialists receive a written description, recommendations and details on confidence levels and event severity to assist in ranking. In addition, EDR Expert enables threat hunting for specific MITRE techniques using a flexible query builder.

3 Manual detection

Threat hunting	• Provides retrospective analysis capabilities for investigating multi-stage attacks even where the data has been encrypted on the hosts, or destroyed by attackers. • Provides automated threat hunting capabilities via IoA engine — enabling the correlation of all events with IoAs generated by Kaspersky's threat hunting team mapped to the MITRE ATT&CK matrix as well as the application of custom IoAs. • Analysts can build complex queries when searching for atypical behavior, suspicious events and threats specific to the infrastructure via a powerful flexible query builder, for proactive threat hunting and to improve the early detection of cybercrime activities. • Analysts can access the Kaspersky Threat Intelligence Portal. Manual threat queries in our Threat Intelligence knowledge base provide IT security analysts with additional context for threat hunting and more effective investigations. • EDR Expert supports threat hunting for individual MITRE techniques using a flexible query builder.
Kaspersky Threat Intelligence Portal access	• Access to the Kaspersky Threat Intelligence Portal is provided directly from the EDR Expert web interface - 1,000 queries a year are included in the license. • The intuitive, easy-to-use interface allows information security specialists to undertake proactive threat hunting and compare the results of internal investigations with global reputation data so they can take the necessary measures to successfully repel attacks quickly.
Send files to the sandbox manually	Files can be sent manually to the sandbox for analysis from the web console by an administrator or an endpoint user. For the cloud delivery option, the license includes 500 queries a year.
Cooperation with external IoC sources and reputation data from third-party Threat Intelligence	Object verdicts from VirusTotal and open threat actor intelligence are supported, providing valuable insights for assessing the potential impact of an incident.

Visibility

Monitoring

Monitoring functions of EDR Expert	• Monitors activities across protected endpoints • Monitors alerts in terms of detection technologies, severity and timeline • Monitors the status of incident handling processes • Monitors threats and attack vectors
Web interface	Provides a visual representation of events, displaying all parent and child events, so incidents can be traced back to their origin, and all effects can be shown.
Endpoint-level extended telemetry collection	The EDR agent collects real-time endpoint telemetry including executable invocations, process creation and changes, registry persistence modifications, file system modifications, network connections and more.
Telemetry exclusions for the EDR agent	Setting telemetry exclusions in an EDR solution allows organizations to customize data collection, conserve resources, and optimize system performance, ensuring security monitoring is aligned with specific needs while minimizing operational impact.

Visualization

The endpoint activity tree and click-down event tree visualization tools enable investigators to easily navigate threat paths by pivoting on key data elements or drill down for more details. Linking events is extremely important for consolidating alerts and providing a complete view of an attack's impact.

Object execution activity tree visualization in the sandbox	Intuitive visualization of emulated object behavior in the sandbox.
Sandbox screenshot management	Relevant screenshots are available straight from the sandbox scan results card, alongside other detonation artifacts.
Query builder for fast search	The solution provides a flexible interface for queries. Fast, real-time query tools provide rapid answers to questions about IoC-type objects and MITRE technique against the centralized data store or against endpoints.
Dashboards	The customizable dashboard interface includes flexible widgets.
Visualization of detects correlation	EDR Expert enables automatic correlation of detects and their visualization in the interface.
Visualization of suspicious / malicious activities	Visualization includes mapping with Kaspersky's unique IoAs, custom IoAs and detection results from Kaspersky Endpoint Security (KES).

Notifications

Incident email notification	The customer can define notifications via email (with customizable severity level).
Severity widget for notifications	The risk level defined for each incident is presented as a severity bar.

Reporting

Report creation	Different types of report can be created and downloaded in HTML and PDF.
Report template customization	EDR Expert can generate its own reports based on customized templates.

Investigation and response

Incident investigation

Processing of incident analysis and incident prioritization	To prevent highly qualified staff from being overburdened and to ensure efficient workload distribution among specialists with different areas of expertise, EDR Expert enables the assessment and classification of threats based on their criticality. Each alert is tagged with an appropriate label, allowing information security specialists to quickly prioritize incidents, focus on the most critical alerts, and effectively allocate resources and plan workloads. Every alert requiring investigation is assigned to a specific information security specialist, with access privileges granted according to the organization's role-based access control (RBAC) model. This approach streamlines incident analysis and response processes while maintaining a comprehensive history of specialist activities and investigation outcomes, enabling detailed reporting.
Centralized investigation	Allows the operator to perform analysis and investigation of multiple endpoints across all endpoints from the single web interface.
Endpoint forensics capabilities	Provides a full set of forensic endpoint data essential for incident investigations: telemetry, collected objects, autorun points, RAM dumps, full disk images, registry key values (within files), process memory dumps, NTFS metafiles and detection results from Kaspersky Endpoint Security (KES), among others.
Retrospective analysis of endpoint activities	EDR Expert visualizes attack stages and provides fast access to retrospective data, which is especially important when compromised endpoints are inaccessible or data has been encrypted by hackers. It helps security specialists to better understand the entire sequence of intruder actions.
Intelligence lookup capabilities	During the investigation process, security specialists have access to the Kaspersky Threat Intelligence Portal, providing them with actionable threat intelligence for additional context.
Offline investigation capabilities	A centralized database stores endpoint telemetry for 30 days by default (scalable) and objects and verdicts indefinitely, so forensic analysis can be performed without relying on the availability of endpoints.

Threat containment

Quarantine of suspicious objects	The specialist can quarantine any object on endpoints to perform investigation actions.
Stop the launch	The specialist can stop the launch of an executable file, document or script in real time either across the entire network or on a specific endpoint.
Host isolation	Any host can be isolated in real time. An IT security expert can specify exceptions by allowing certain inbound and/or outbound network traffic directions that should not be blocked.

Response activities

Endpoint-level prevention	File / script / Office document execution can be prevented on endpoints through customer-defined rules.
Prevention with Kaspersky Endpoint Security (KES)	When sharing a single agent with Kaspersky Endpoint Security (KES), the product provides ML-based high-end prevention capabilities covering advanced pre-execution protection: • Common threat blocking • Exploit prevention • Fileless malware prevention • Ransomware prevention • Credentials theft protection • Protection for servers
Auto prevention	The launch of files on all hosts can now be automatically prevented when a sandbox detect occurs, according to established auto-response rules.
Kill process / service	Any process / service can be remotely killed on an endpoint to contain the threat and to block data exfiltration and lateral movement attempts in real time.
Remote program execution	Any additional software can be run remotely on a selected endpoint machine.
Commands execution on the host	Any commands can be run remotely on a selected endpoint machine.
Delete object from endpoints	Objects can be remotely deleted from a single endpoint or a group of machines.
Block list updates in KPSN	Verdicts are automatically added in the block list in Kaspersky Private Security Network to enable real-time sharing with other Kaspersky products.
Guided response	Recommendations are categorized under four types of action: **Qualifying** — depending on the type of alert, may include: • Lookup in Kaspersky Threat Intelligence Portal by hash • Show sandbox report • Find related alerts by host name, URL or IoC • Find KES event **Containment** — depending on the type of alert, may include: • Host isolation • Create prevention rule • Create task **Investigation & response —** depending on type of alert, may include: • Find related events • Save alert indicators as IoA **Close** — depending on the type of alert, may include: • Restore from quarantine • Enable isolated hosts • Delete prevention rules

Recovery

File recovery from quarantine	During quarantine, any object can be recovered back to the endpoint by the specialist at any time.
Enable isolated hosts on the network	Isolated hosts can be enabled on the network by the specialist at any time.
Rollback	Kaspersky Next EDR Expert provides a rollback procedure that protects different objects, including files, registry keys, tasks, etc. After detection, the rollback mechanism restores the user's data and also deletes the created registry key.

Administration

Health check of modules	Health-check information is displayed in the web interface, with its status available through a dedicated widget.
Notification of system errors	Email notifications about operational problems with system components can be configured directly from the EDR Expert web interface.
Agent management	EDR Expert uses Kaspersky Security Center through a special plug-in, enabling the installation and removal of agents, as well as handling updates, configuration, status monitoring (reports) and endpoint tracking — with and without a standalone EDR Expert / KES agent.
Agent control	EDR Expert's web interface provides security specialists with the following information: • List of endpoints with EDR Expert agents • Endpoint information: OS, name, IP address, etc. • Agent version • Agent status: error, license status, time of last connection, etc.
Autodeletion of inactive hosts	Auto-deletion of inactive hosts within lists of EDR agents on the server helps to optimize resource usage, reduce noise and alert fatigue.
Multi-tenancy architecture support	EDR Expert supports multi-tenancy architectures to protect the infrastructure of several tenants (organizations) simultaneously.
Distributed installation	Connection of up to 150 Secondary Central Nodes to a Primary Central Node (MSSPs and large enterprises).
Lowered system requirements for small installations	Sizing guides for smaller installations supporting multitenancy are also included.
Subscription licensing	Subscription licensing is available for Managed Security Service Providers (MSSPs).
Password polices	Allows enforcement of mandatory account password changes.

Integration capabilities

External Indicators of Compromise (IoCs) upload	IoCs can be imported in OpenIOC format for use in infrastructure searches.
Integration with SIEM	Alerts can be exported in CEF format and imported into the SIEM for correlation with information from other log sources.
Deep integration with Kaspersky Endpoint Security (KES)	Kaspersky Next EDR Expert provides high-end ML-based prevention capabilities covering advanced pre-execution protection. Data from Kaspersky Endpoint Security (KES), including detection, blocking, and suspicious event information, is directly accessible through EDR Expert. This enhances threat investigations by enabling the detection of complex attacks and supporting informed decision-making.
Integration with third-party antiviruses	Users can now use EDR agents for Windows alongside various antivirus solutions simultaneously.
Integration with KPSN to support the local verdicts database	Verdicts from the EDR Expert are stored on the local KPSN blocklist and automatically transferred via KPSN to other installed Kaspersky products, including Kaspersky Endpoint Security (Kaspersky Security for Windows Servers), Kaspersky Hybrid Cloud Security, Kaspersky Security for Storage, etc.
API for sending alert information to external systems	EDR Expert provides an API that lets external systems access information about all program alerts.
Send telemetry to third-party via API	EDR Expert provides an API that lets external systems access information about all program telemetry.

Find out more about Kaspersky Next EDR Expert

Kaspersky Next EDR Expert

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture