



Product White Paper

Kaspersky Next XDR Expert

kaspersky bring on
the future

Contents

Existing challenges and threats to an organization's information security	3
About Kaspersky Next XDR Expert	4
Functional comparison of the Kaspersky Next tiers	6
Solution's architecture	8
Breakdown of functionality	8
Automated protection of physical and virtual endpoints from mass threats	
Advanced detection and response to complex threats at the endpoint level	
Cross-correlation engine for data collection, normalization, monitoring and correlation	
Incident response and case management	
Investigation and proactive search	
Response automation and orchestration	
Hybrid cloud security	
Security for mail servers	
Dashboards and reporting	
Integration capabilities	
Why choose us?	18

Existing challenges and threats to an organization's information security



XDR's ease of use **in detecting common threats** reduces the need for in-house expertise and **reduces the manpower** required to operate disparate security solutions from different vendors.



To protect valuable data, systems and reputation, enterprises need a proactive approach that incorporates advanced technologies, strong policies, vigilant monitoring and training.

To combat sophisticated targeted attacks such as APTs, cybersecurity personnel must manually analyze and assess a large number of incidents while performing challenging tasks in an understaffed setting. Additionally, they must use information security tools that are managed via separate consoles and do not communicate with one another.

This lack of a consolidated, unified view of information leads to poor decision making, making it difficult to identify and respond to situations, while the volume and complexity of attacks, the expanding attack surface, and the global shortage of skilled cybersecurity professionals make it difficult to stay ahead of the adversary. It is noteworthy that 77% of companies experienced at least one cyber-incident in the past two years, with many suffering up to six in the same period*.

Organizations should strive to reduce the time it takes to detect and respond to an incident to minimize the risk of a successful attack in the first place, and, if an incident does occur, to reduce the time, manpower, and, therefore, monetary costs required to recover from a cyberattack.

For organizations that do not use specialized cyberdefense solutions, detecting complex threats that require the collection, storage and analysis of data, as well as the various stages of investigation and response can be extremely labor-intensive without the use of automation, while 41% of InfoSec professionals surveyed say their organization's cybersecurity teams are "somewhat" or "significantly" understaffed. The biggest challenges in finding and hiring the right InfoSec professionals are discrepancies between certification and practical skills, and a lack of experience**.

Using multiple tools simultaneously also increases manual operations and is likely to lead to inefficient, overloaded security operations and additional costs.

Specialized Extended Detection and Response (XDR) solutions are recommended for security teams to automate routine processes, increase the efficiency of the entire cycle of complex incidents, and reduce the time it takes to process complex incidents and the time to detect (MTTD) and respond (MTTR) to complex attacks. These solutions typically integrate a range of advanced technologies.

* Kaspersky Human Factor 360 Report, 2023

** Kaspersky Report: The portrait of modern information security professional, 2024



Kaspersky Next XDR Expert



Open Single Management Platform

About Kaspersky Next XDR Expert

The ultimate cybersecurity tool for proactive defense against cyberthreats

As the most advanced tier of the Kaspersky Next product line, we offer a robust cybersecurity solution that defends against sophisticated cyberthreats, providing full visibility, correlation and automation, leveraging a diverse range of response tools and data sources, including endpoint, network and cloud data.

Kaspersky Next XDR Expert provides an all-encompassing view of a company's security, ensuring that no potential threat goes unnoticed. Easy to deploy and manage, Kaspersky Next XDR Expert is backed by advanced analytics capabilities and a strong track record of security expertise.

We offer an Open XDR solution with an **Open Single Management Platform** – the next step in the evolution of Kaspersky Security Center and a universal tool for creating a unified ecosystem of cybersecurity products.

At the core of Kaspersky Next XDR Expert is the functionality of our leading solutions – Kaspersky Unified Monitoring and Analysis Platform (SIEM), Kaspersky Next EDR Expert, Kaspersky Hybrid Cloud Security and Kaspersky Security for Mail Servers. In addition to the above products, other integrations can be added on demand to customize the platform for the specific needs of an organization (NDR, OT, TI, Awareness, etc.).

Besides the main Kaspersky Next XDR Expert offering, **our solution is also available as Kaspersky Next XDR Core for customers who already have an EDR solution** and do not want to repurchase:

1

Kaspersky Next XDR Expert

combines best-in-class endpoint protection, mail and hybrid environment security with the advanced detection capabilities of Kaspersky Next EDR Expert, a correlation engine and automated responses. Third-party connectors can be added to pull all the data together.

2

Kaspersky Next XDR Core

is for customers who already have endpoint and EDR solutions in place and don't want to repurchase them, preferring to extend the functionality with a correlation engine, automated responses and third-party connectors.

Key solution capabilities:



Comprehensive threat detection. Identify sophisticated threats, including malware, ransomware and advanced persistent threats (APTs) by cross-correlating telemetry from Kaspersky and hundreds of third-party vendors.



Automated and manual response. Leverage predefined and user-created playbooks to automate typical response operations, speed up MTTR and minimize errors in frequently occurring situations.



Endpoint protection integration. Prevent attacks with integrated EPP functionality to neutralize mass attacks and free analysts to focus on complex threats. We also provide cybersecurity training for IT administrators, security for MS O365, and unlimited sandbox functionality.



Threat intelligence and contextual data. Use comprehensive threat intelligence based on Kaspersky data to provide contextual information about threats and attackers, enabling quick and accurate response and minimizing false positives upon detection*.



Integration capabilities. Benefit from capabilities such as automation, full visibility and awareness without having to replace third-party security solutions.



Data lake. Leverage our centralized local repository that provides a platform for collecting, indexing and analyzing logs from various sources with advanced search functionality across storage areas, as well reporting and threat hunting capabilities.



Compliance and regulatory support with data sovereignty. Use reporting and auditing capabilities that facilitate compliance while keeping data confidential within your company's perimeter.



Built-in, unlimited, advanced sandbox. Use a safe environment for deep analysis of threat activity.






Monitor and respond across the entire hybrid infrastructure. whatever the workload – physical, virtualized, or based in private, public or hybrid clouds.



Easily monitor and respond across all levels of **corporate mail security**.

* The offering includes 50 free Kaspersky Threat Lookups. Data feeds are available via integrations and purchased separately.

Functional comparison of Kaspersky Next tiers

				
		Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
Automated protection of physical and virtual endpoints	Multi-layered anti-malware	•	•	•
	Behavior detection	•	•	•
	Exploit prevention	•	•	•
	Remediation engine	•	•	•
	File, mail, web and network threat protection on endpoint level	•	•	•
	Firewall	•	•	•
	Host Intrusion Prevention (HIPS)	•	•	•
	AMSI protection	•	•	•
	BadUSB attack prevention	•	•	•
	Root cause analysis with an alert card	•	•	•
	Global threat intelligence via Kaspersky Security Network	•	•	•
	Mobile threat defense (Android, iOS)	•	•	•
Supported OS	MacOS, Linux, Windows	•	•	•
System hardening and IT training	Vulnerability assessment	•	•	•
	Hardware and software inventory	•	•	•
	Application, web and device controls	•	•	•
	Mobile device management (MDM)	•	•	•
	Remote troubleshooting	•	•	•
	Third-party apps & OS installation	•	•	•
	Patch management		•	•
	Remote wipe		•	•
	Encryption management		•	•
	Cybersecurity training for IT administrators		•	•
Cloud security	Cloud discovery	•	•	•
	Cloud blocking		•	•
	Data discovery		•	•
	Security for Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams		•	•
Advanced detection and response to complex and persistent threats	Indicators of compromise (IoCs) search and threat hunting with automatic cross-endpoint response		•	•
	Adaptive anomaly control		•	•
	Single-click and guided response		•	•
	System critical object check		•	•
	Move file to quarantine / Recover file from quarantine		•	•
	Network isolation / remove network isolation		•	•
	Get / delete file		•	•
	Start / terminate process		•	•
	Critical areas scan		•	•
	Execution prevention		•	•
	Execute command		•	•
	Endpoint telemetry collection		•	•
	Proactive threat hunting and retrospective analysis		•	•
	Advanced detection with indicator of attack (IoA)		•	•



Kaspersky Next
EDR Foundations



Kaspersky Next
EDR Optimum

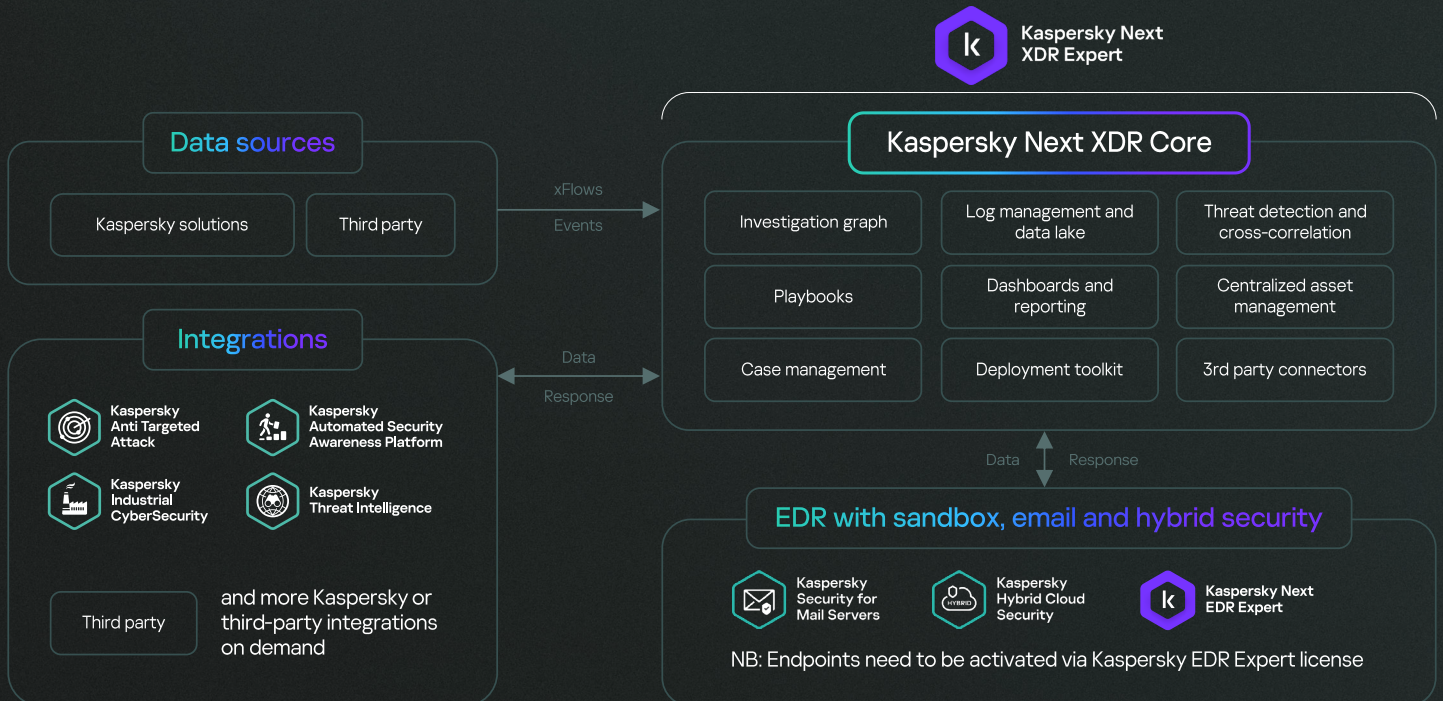


Kaspersky Next
XDR Expert

Advanced detection and response to complex and persistent threats	YARA rules (Windows only)			•
	MITRE ATT&CK mapping		•	•
Built-in advanced sandbox	Multi-level assessment and behavior analysis of emulated objects		•	•
	Managing virtual machine templates		•	•
	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		•	•
Service management	Start / stop / delete / pause / resume service		•	•
	Modify startup type of service		•	•
Forensics (Windows only)	Process lists		•	•
	File list		•	•
	Autorun list		•	•
	Process memory dump		•	•
	Memory dump		•	•
	Disc image		•	•
	NTFS service files		•	•
	Registry key		•	•
Email security	ML-based malware, spam and phishing detection			•
	Various deployment options (SEG, cloud, standalone)			•
	Content filtering			•
	Mail sender authentication using SPF, DKIM and DMARC			•
	Integration capabilities			•
	Expanded data export to SIEM			•
Hybrid cloud security	File integrity monitoring (FIM)			•
	Log inspection			•
	Private cloud support: VMware, Red Hat Enterprise Linux, KVM			•
	Public cloud support: Google Cloud, Microsoft Azure, AWS			•
	VDI platforms support: VMware, TERMIDESK, Citrix			•
Threat intelligence enrichment	TI enrichment (50 Threat Lookups)		XDR Core	•
Extended detection and response capabilities	Investigation graph			•
	Incident response and case management			•
	Playbooks: Response automation and orchestration			•
	Deployment toolkit and Open API			•
Cross-correlation engine for data collection, normalization, monitoring and correlation	250+ third-party connectors			•
	Dashboards and reporting			•
	Log management with data lake			•
	Advanced threat detection and cross-correlation			•
	Alerts aggregation and asset management			•

Solution architecture

Act quickly and make the right decisions using the best security products, seamlessly integrated into Kaspersky Next XDR Expert.



Breakdown of functionality



More features

The solution comes with dashboards and reporting, Open API, deployment toolkit, 50 free Threat Lookup requests, as well as monitoring and response capabilities in hybrid cloud environments and corporate email networks. Upon request, the solution can be integrated with a range of Kaspersky or third-party solutions: NDR, OT, Threat Intelligence, Security Awareness and more on demand.

The solution covers the following areas of cybersecurity **out of the box**:

- 1 Automated protection of physical and virtual endpoints from mass threats
- 2 Advanced detection and response to complex threats at the endpoint level
- 3 Cross-correlation engine for data collection, normalization, monitoring and correlation
- 4 Incident response and case management
- 5 Investigation and proactive search
- 6 Response automation and orchestration

Automated protection of physical and virtual endpoints from mass threats

Protecting business systems from a vast array of advanced persistent threats with enterprise-grade malware protection, ransomware protection, and constant endpoint monitoring.

To strengthen an organization's cyberdefenses, each security stage, starting with prevention, must be accelerated and maximized. That is why our XDR solution includes advanced but easy-to-use and intuitive endpoint protection that frees up the resources of security professionals to tackle complex tasks.



The solution keeps company data secure with industry-proven anti-ransomware and anti-malware tools; prevents known and unknown malware threats from infecting corporate devices with robust protection against file, web and mail threats; and monitors which applications on corporate endpoints need updating with routine vulnerability scanning. The platform supports Windows, Linux and iOS, as well as Android and iOS mobile devices.



Kaspersky Next XDR Expert employs strong app, web and device controls to protect users on the network from external threats, detects and roots out advanced attacks on the network and provides a visual path with comprehensive root cause analysis. In addition, the platform alerts the administrator to any suspicious activity or security holes on the protected network with cloud discovery and vulnerability assessment.

Advanced detection and response to complex threats at the endpoint level

Unparalleled threat visibility with rapid investigation and guided response mechanisms that adapt to quickly thwart new threats.

The solution includes streamlined EDR with powerful endpoint protection to provide a simple and robust defense against a wide range of threats. This allows the security team to gain visibility into threats and learn their paths on the endpoint, with the ability to **quickly and painlessly perform root cause analysis on all the gathered data** – while the investigation graph of our XDR platform gives security teams access to a variety of data beyond the endpoint.

The EDR capabilities of our XDR platform enable organizations to confidently stop threats in their tracks with guided response and automation, while helping **uncover their traces across endpoints with indicators of compromise** generated from an investigated alert or imported from a trusted source.

All this helps to automate the reduction of the attack surface with enterprise-grade controls. Kaspersky also offers integrated **cybersecurity training for IT staff**, empowering them to help detect threats and collect valuable data.

Cross-correlation engine for data collection, normalization, monitoring and correlation

Log management with data sovereignty for regulatory compliance and incident investigation

Kaspersky Next XDR Expert includes a **centralized platform for collecting, indexing and analyzing logs** from various sources to provide full visibility of the entire infrastructure and reduce false positives. This includes information security tools (DLP, NGFW, VPN, IDS, business applications and security tools, etc.) and the use of that data for detection. Integration of external event sources is available on demand with free creation of additional connectors by Kaspersky Professional Services.

The platform provides **efficient data compression during data storage**, saving significant disk space without compromising search speed or capabilities. Information can be stored locally or in a private data center. Different levels of data storage levels are supported, allowing data to be stored in “hot” and “cold” access. This allows the administrator to flexibly manage the cost of hardware resources required to store events. It is important to note that the user does not need to consider the storage areas when forming search queries: access to the necessary area is provided by internal mechanisms of the platform, while experts can use a single interface to execute search queries and focus entirely on the investigation. **As a result, the cost of ownership of the system is reduced compared to legacy vendors and the quality of the user experience remains high.**

By collecting and storing logs from a variety of sources, organizations can **meet regulatory requirements** related to data retention, auditing and incident investigation, and centralized and structured storage allows organizations to easily retrieve and analyze logs as needed.

>500

preconfigured rules for detecting attack scenarios, which are regularly updated with MITRE mapping and response recommendations.



The platform uses historical data to identify trends, find previously unidentified threats, and pinpoint attacks overlooked by certain security elements, all of which improve the overall effectiveness of threat detection. By adjusting product settings, the user can control the process and obtain events and telemetry. The correlation process includes analysis of contextual information (assets, accounts – more on this below), global threat intelligence and more to reduce false positives and improve detection rates.

Real-time and historical correlation of security events

Kaspersky Next XDR Expert allows you to **cross-correlate security events** in near real time using customizable rules for identifying attacks and threats, as well as hundreds of predefined rules developed by Kaspersky SOC, one of the most successful and experienced active threat hunting teams in the industry. Kaspersky SOC experts hold numerous certificates confirming their high level of expertise and knowledge.

Centralized asset management

This functionality reduces false positives, provides updates for vulnerable nodes and creates a **customized asset model with an array of metadata** (hardware, OS, installed applications, vulnerabilities, IP addresses, etc.). The platform uses Kaspersky endpoint data during installation and then supports import of asset data from various sources (vulnerability scanners, CMDB, etc.).

This asset management approach involves inventorying all endpoints, servers and network devices and assessing their importance in order to improve visibility and help prioritize alerts.

* 5 log parsers are included by request with the MSA Business Certificate/Premium license/Successive Plus license. 10 log parsers by request are included by request with the MSA Enterprise Certificate/Premium Plus license. The Premium license and Premium Plus license will be the only options available in 2025.

Incident response and case management

Case management for coordinating incident response activities

Kaspersky Next XDR Expert incident management provides a centralized workspace for analysts and **improves the ability of security teams to identify and investigate incidents**, boosts the effectiveness of alert processing, and makes a coordinated response easier. Security analysts can use the platform to tag incidents using the **MITRE ATT&CK matrix**, prioritize alerts, enrich data, and initiate response actions.



The process begins by searching, editing and preprocessing the data. Telemetry is enriched and response actions can be triggered manually or automatically.



The user is then assigned an alert or incident and its status changes. Several incidents can be combined into one, and there is also an option to leave comments.

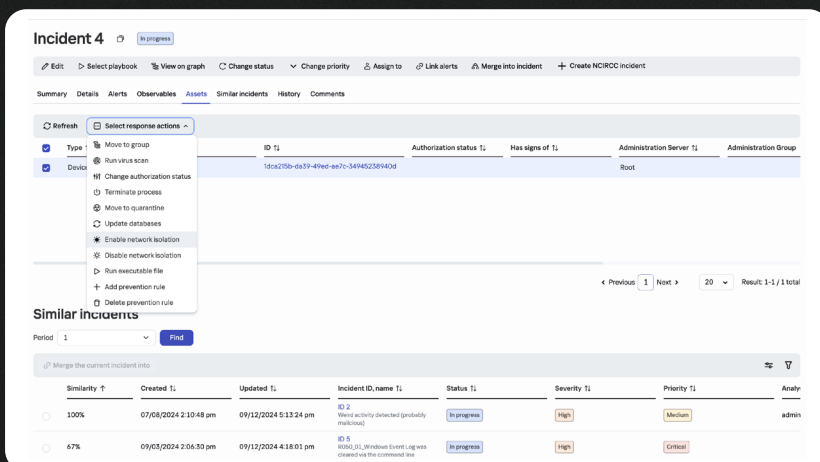


The analyst can then manually delete the alert in the incident, create an incident from the alert, or link the alert to an incident and proceed to the investigation column.

The **Kaspersky Threat Lookup*** online platform will enable users of Kaspersky Next XDR Expert to obtain comprehensive details about detected threats and their relationships, while the Kaspersky CyberTrace platform's enrichment events, based on real-time threat data feeds, will automate the prioritization process.

Purchasable feeds support data sovereignty by providing a locally available source of feed enrichment that includes:

- Malicious URL
- Phishing URL
- IP reputation
- Malicious hashes
- Botnet C&C URL
- Ransomware URL
- and more.



The product interface has an "Incident" section that can be used to coordinate the joint work of several analysts. The incident card helps to collect all the data about each case in one place.

* The offering includes 50 free Kaspersky Threat Lookups. Data feeds are available via integrations and purchased separately.

Investigation and proactive search



Provides a holistic view of the threat landscape, focusing on incidents as a whole rather than individual alerts.

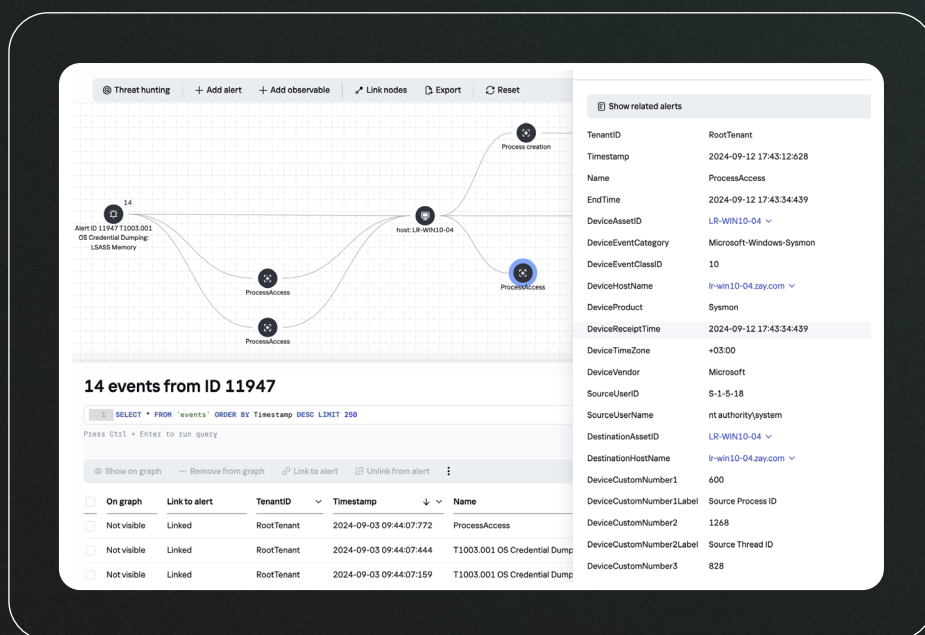
Supports collaborative incident investigation with the ability to save “progress” in the graph and share with colleagues for later analysis.

The investigation graph saves analysts time when building the attack chain by eliminating gray areas. It also helps reconstruct a complete picture of an incident using data from third-party sources and serves as a tool for **collaborative incident investigation**. A single investigation graph can store the progress of an investigation, allowing users to complete their part of the investigation and pass the link to another analyst for further action. Analysts can edit the graph manually, search for missing items using event search, and add relevant events to the graph.

The investigation graph focuses on the entire incident, not just individual alerts

An investigation graph is a powerful visual analysis tool that **shows the relationships between events, alerts, incidents, assets and other objects**. It allows security teams to get a complete view of an attack and quickly find the root cause of attacks, using all the relevant information.

It saves time by **combining data** from Kaspersky Threat Intelligence, incidents, alerts, events, EDR telemetry and contextual enrichment to quickly build an attack chain. With this tool, complex attacks with lateral movement (when hackers infiltrate a single node and begin exploring it, gradually destroying the infrastructure as they search for their targets) can be detected and investigated in the shortest possible time.



Provides a **holistic view of the threat landscape** with a focus on specific incidents.



Allows you to quickly **find the root cause of attacks** and obtain important information.



Helps reconstruct a **complete picture of an incident** using data from third-party sources.



Saves analysis time when building the attack chain by eliminating gray areas.

Response automation and orchestration

A set of playbooks provides advanced functionality for automating incident response workflows using preconfigured and custom scripts.

This feature of Kaspersky Next XDR Expert allows security teams to automate incident response processes using predefined and custom scripts (playbooks). To respond to alerts or incidents, playbooks use an algorithm consisting of a sequence of response actions that help analyze and process alerts or incidents.

Monitoring & reporting / Playbooks

Tenant filter: 4 selected

+ Create Duplicate and edit Edit Delete

Name ↑↓	Operation mode	Tags	Actions	Launches ↑↓	Modified ↑↓	Created ↑↓
[KL] P001 "Creation of executable files by office applications"	Manual	Predefined	1. assignKasapGroup 2. resetLDA	1	07/04/2024 5:37:25 pm	07/04/2024 5:37:
[KL] P002 "Windows Event Log was cleared"	Manual	Predefined	1. blockLDAPAccount	4	07/04/2024 5:37:25 pm	07/04/2024 5:37:
[KL] P003 "Suspicious child process from wmiprvse.exe"	Training	Predefined	1. avScan 2. blockLDAPAccount	0	07/04/2024 5:37:25 pm	07/04/2024 5:37:
Run 3rd-party script	Manual		1. executeCustomScript	0	08/28/2024 4:12:04 pm	08/28/2024 4:12:

< Previous 1 Next > 20 Result: 1-4 / 4 total

The user can configure automatic or manual playbook startup. These are the following types of operation modes:



Auto

A playbook in this mode launches automatically when appropriate alerts or incidents are detected.



Training

A playbook in this mode prompts the user for permission to launch when appropriate alerts or incidents are detected.



Manual

A playbook in this mode can only be launched manually.

These scenarios cover all integrated solutions such as Kaspersky Next EDR Expert or Threat Intelligence, as well as third-party products. We offer a set of preconfigured integrations that can be customized and extended, allowing our XDR platform to be tailored to the needs of each customer.

Playbooks speed up routine operations, free up security professionals for more complex investigations, and help minimize errors in common situations, increasing the speed and accuracy of incident response.

Hybrid cloud security

Proven cloud-native protection and best performance for your hybrid environment

Cloud computing has become commonplace, and the majority of businesses employ hybrid cloud deployments that combine on-premises and cloud (public or private) environments. The cloud offer many benefits to businesses, including increased agility and flexibility. However, there are also drawbacks, such as sudden increases in infrastructure complexity, costs, and performance inefficiencies.

Our Kaspersky Next XDR Expert provides **multi-layered threat protection for hybrid infrastructures**, including physical, virtualized, and private, public, or hybrid clouds. It proactively detects malware, phishing, and other cyberattacks, reducing the need for manual tasks to ensure compliance.

1

Machine learning algorithms backed by human expertise deliver the highest levels of detection with minimal false positives.

2

The solution includes File Integrity Monitor (FIM) and Log Inspection

3

Private cloud support: VMware, Red Hat Enterprise Linux, KVM

4

Public cloud support: Google Cloud, Microsoft Azure, AWS

5

VDI platforms support: VMware, TERMIDESK, Citrix

6

Real-time threat intelligence helps defend against the latest exploits.

7

Response actions such as host isolation and de-isolation can be manual or automated.

8

Light agents optimized for each OS efficiently reduce consumption of virtualization resources by up to 30% in private clouds, freeing them up for use in other areas of the business.

Security for mail servers

Comprehensive email security for free-flowing business communications

To facilitate effortless monitoring of all levels of corporate mail security, we are adding Kaspersky's unique stack of protection technologies, proven by regular independent testing, into our Next XDR Expert solution. As well as **gateway, mailbox and cloud email security**, protection for MS365 apps, ML-based malware, and spam and phishing detection, the new additions include:

1

Response actions such as blocking by email or IP address, attachment analysis that can be performed manually or automatically

2

Complex regular expression filtering and confidential document templates to mitigate the risk of data leakage, reinforcing overall protection

3

In-depth **analysis of attachments within a secure, emulated environment**

4

Identification of unwanted emails using sender attributes, IP addresses, message size and headers. Unique image signatures and analysis of message content and attachments to detect new spam threats quickly.

5

Advanced machine learning to handle diverse threat scenarios, from widespread phishing to sophisticated spear phishing.

6

Multi-level defense powered by deep learning neural networks to **quickly stop complex email threats**, including non-standard Trojans and targeted ransomware attacks.

7

Mail sender authentication using Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).

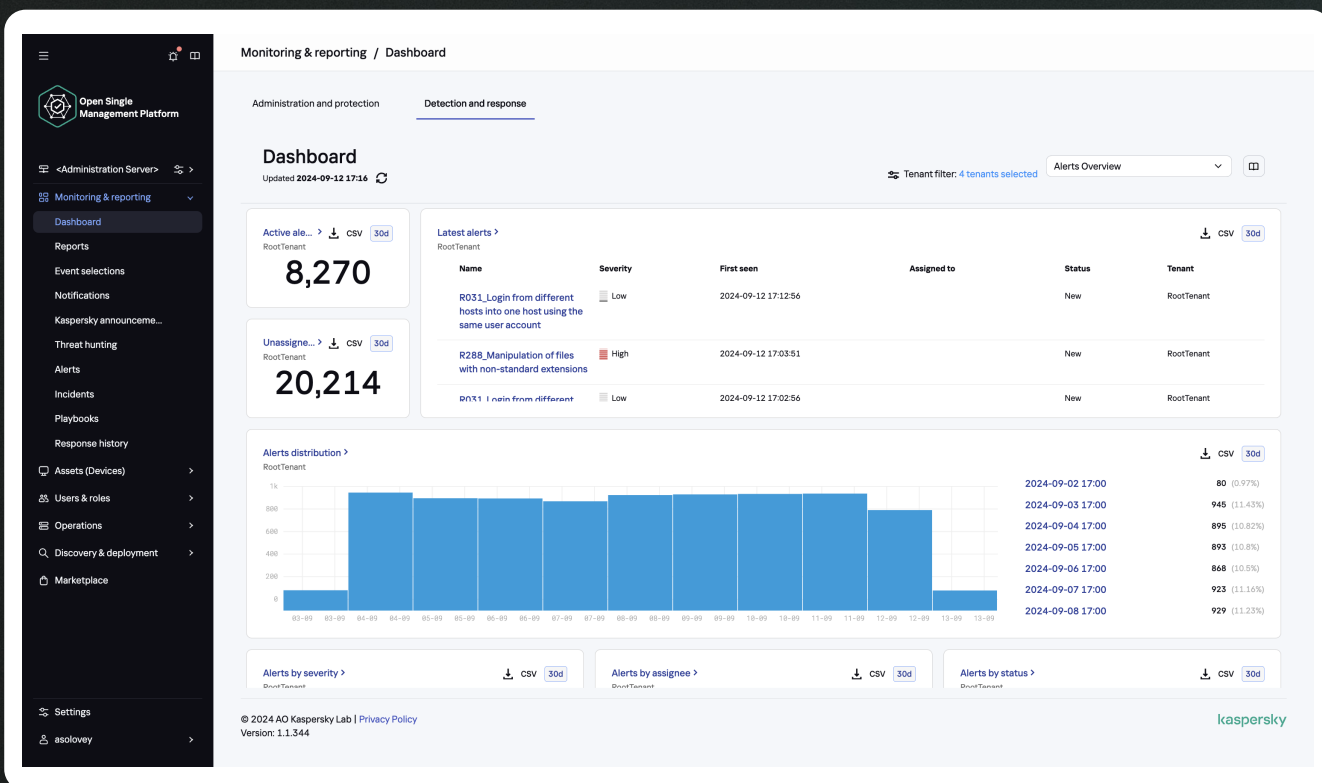
8

A separate Kaspersky Anti Targeted Attack protection widget is located in the dashboard, which displays various statuses or emails processed by our advanced sandbox.

Dashboards and reporting

Comprehensive data on the protected infrastructure that empowers security specialists and facilitates effective incident response

The monitoring dashboard allows analysts to assess the overall information security status of the infrastructure and track the effectiveness of security operations. Kaspersky Next XDR Expert's detailed data analysis and reporting capabilities allows for the automated the creation of an up-to-date snapshot of the enterprise's security situation at various monitoring levels: CEOs, managers and security analysts.



The platform allows users to create their own widgets and graphical panels with different settings relevant for different types of data.

Integration capabilities

Extensive integration capabilities with support for various cross-product scenarios

Kaspersky Next XDR allows data (logs) to be received from other systems and devices, and the customization of automatic responses in third-party products. The solution includes a wide range of ready-made integrations with both Kaspersky products and products from other vendors. It is also possible to add additional integrations that can be developed by Kaspersky Professional Services, partners or customers (including using API capabilities of plug-in products).



By security domain

- Endpoint Protection (EPP & EDR solutions)
- Email and web traffic protection (email protection, NDR, FW/NGFW, UTM, IDS)
- Security Awareness
- Cloud workload (CASB, CWPP)
- Threat Intelligence (CTI)
- Identity Security (IAM, PAM)
- OT / IoT Security
- Data loss prevention (DLP)



By data type

- XML
- Syslog
- CSV
- JSON
- SQL
- IPFIX
- CEF
- NetFlow v5
- NetFlow v9
- Key-Value
- RegExp



By transport type

- TCP
- UDP
- NetFlow
- sFlow
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse)
- File
- Diode
- FTP
- NFS
- WMI
- NATS JetStream
- Kafka
- HTTP
- WEC
- SNMP
- SNMP Traps
- VMware API

[Full list](#)


By vendor (200+ sources supported out of the box)

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- Eclectiq
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler

[Full list](#)

Why choose us?



Reduce total cost of ownership with a scalable solution based on **modern technologies** such as microservices and REST API. Kaspersky Next XDR Expert makes it easier to deploy solutions using modern and efficient development approaches, eliminating the need to carry decades-old legacy systems.



Our stack of technologies for both industrial and corporate sectors allows us to provide **Single IT-OT XDR** for customers who want to work with actionable data from both environments.



We are one of the few vendors that can offer **data sovereignty without compromise** with our on-premises installation and operation in isolated perimeters, guaranteeing the confidentiality of customer data processing.



We have **200+ preconfigured integrations** and we are adding more. With built-in integrations we can receive data from various solutions (DLP, NGFW, VPN, IDS, business applications and security tools, etc.) and use that data for detection. Integration of external event sources is available on demand with free creation of additional connectors.



Seamless and tight integration between Kaspersky products reaches a level unattainable by third-party solutions, boasting a unified support system and seamlessly integrated design.



To ensure XDR covers all stages from prevention to investigation, we have built our solution on top of **the best-in-class Kaspersky EDR**, which stands out on a global scale with awards and active participation in international bodies such as Interpol and MARR.



Kaspersky Extended Detection and Response (XDR) has received **Leader status from ISG** (Information Services Group) for the second year in a row, reaffirming its technological excellence and ability to combat new and complex threats.

[Learn more](#)



**Kaspersky Next
XDR Expert**

www.kaspersky.com

© 2024 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

[Learn more](#)

#kaspersky
#bringonthefuture