Kaspersky Next XDR Expert

Unparalleled insight. Total protection.

kaspersky

The complexity of businesses cybersecurity

The cyberthreat landscape makes it extremely challenging for organizations to stay on top of their cybersecurity while focusing on core business operations. Add an ever-expanding attack surface, regulatory requirements, and the global skills gap to the mix and it's easy to see why modern businesses are under so much pressure — and why so many cyberattacks succeed.

51%

of companies struggle to detect and investigate advanced threats with current tools

68%

of companies experienced a targeted attack on their networks and suffered data loss as a direct result

$6 trillion

per year: the global annual cost of cybercrime

400 000

new pieces of malware are detected every day

Sources: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Complete visibility. Unmatched protection.

As part of the Kaspersky Next product line, we have introduced Kaspersky Next XDR Expert, a solution that embodies Kaspersky's XDR approach and provides an all-encompassing view of a company's security.

Kaspersky XDR is a robust cybersecurity solution that defends against sophisticated cyberthreats. It provides full visibility, correlation & automation, leveraging a diverse range of data sources, including endpoint, network and cloud data.

It evolved from Kaspersky Anti-Targeted Attack platform as Native XDR in 2016 to Open XDR in 2023, providing an all-encompassing view of security. Easily managed from the Open Single Management Platform, Kaspersky XDR offers a comprehensive on-premise security, ensuring that customers' sensitive data remains within their own infrastructure while meeting data sovereignty requirements.

Open XDR

Open XDR solutions are designed to work with a wide range of security products, allowing organizations to integrate various security products from different vendors, offering more flexibility and vendor-agnostic capabilities.

Native XDR

Native XDR solutions typically work seamlessly with the vendor's own ecosystem of security tools, providing a more unified and cohesive experience. These solutions are purpose-built to work together, offering deep integration, automation, and streamlined workflows within the vendor's security product suite.

Key technologies

We offer Open XDR as a single open platform — a universal tool to create a unified ecosystem of cybersecurity products. At the core of Kaspersky XDR are our leading solutions — Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations and Kaspersky Endpoint Detection and Response Expert. For advanced network management, KATA is an additional option.

Monitoring and Analysis

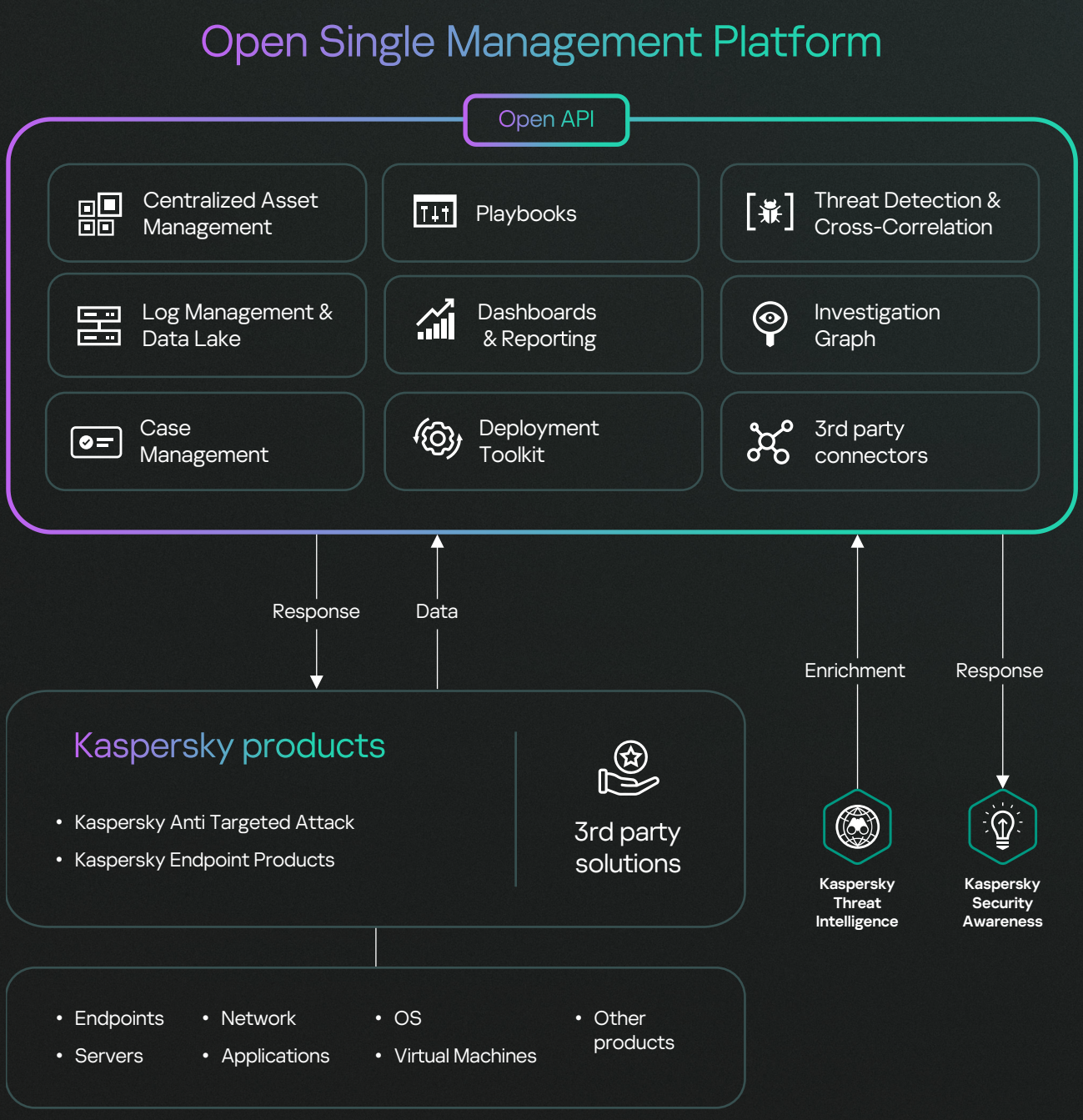
Provides centralized collection and analysis of logs, correlation of security events in real time and timely notification of incidents. Includes a ready-made set of correlation rules and access to the rich portfolio of Kaspersky Threat Intelligence services to identify and prioritize threats, attacks and IoCs.

Endpoint Protection

Delivers robust endpoint protection, protecting against ransomware, malware and fileless attacks. On-premise or in the cloud, our endpoint protection uses machine learning and behavior analysis to protect all types of endpoints running any major OS.

Endpoint Detection and Response

Delivers comprehensive visibility and superior defenses across all an organization's endpoints. Enhanced threat hunting and discovery thanks to Kaspersky's unique, wide-ranging threat intelligence, plus automation of routine tasks, guided investigation processes and customizable detections all promote quick incident resolution.



Powerful features, significant benefits

Real-time data fusion from third parties

The capability to integrate data from third-party sources extends beyond just endpoints and is enhanced by real-time cross-correlation.

Automated Response and Remediation

Quarantine or isolate compromised endpoints, block malicious activities, and remediate vulnerabilities, reducing manual effort and response time.

Best-in-class EPP / EDR

Recognized as the global leader, Kaspersky sets the benchmark for EPP / EDR solutions worldwide. Kaspersky EDR excels on a global scale, backed by awards and active participation in international committees such as Interpol and MAPP.

Unrivaled scalability

Capable of supporting loads encompassing hundreds of thousands of endpoints on a single instance, Kaspersky XDR diligently tracks threats in real-time while ensuring high availability.

Data sovereignty

Kaspersky XDR is one of the few vendors offering a comprehensive onpremise XDR solution, ensuring customers' sensitive data remains within their own infrastructure while meeting data sovereignty requirements.

Seamless & tight integration across Kaspersky products

Interaction between products reaches a level that remains beyond the reach of third-party solutions, boasting a unified support system and seamlessly integrated design.

Multi-tenancy that enables MSSP scenarios

Provide XDR as a service with full-fledged tenants — users of one tenant cannot see the data of other tenants, while the main admin (the MSSP) can build detection and response processes for all clients.

Advanced security scenario customization and infrastructure-wide data analysis

Empowering users to configure intricate security scenarios with the added ability to analyze data across their entire infrastructure.

Integration capabilities

The wide range of integrations which work with Kaspersky XDR provides a unified and contextualized view of potential threats, giving your security team all the tools and information they need to protect your organization from whatever cybercriminals throw at you.

The product's integration capabilities encompass the ability to receive data (logs) from other systems and devices, as well as to set up automated responses in other products. Kaspersky XDR comes with a wide range of out-of-the-box integrations, with Kaspersky and third-party products. It's also possible to add additional integrations which can be developed either by Kaspersky Professional Services or by partners or customers themselves (including using the API capabilities of connectable products). Integration is possible with systems from various domains and different vendors, and numerous protocols and data formats are supported.

By security domain

Endpoint Security

- EPP & EDR solutions

Network & Web & Email Security

- Email Protection
- Network Detection and Response (NDR)
- Firewalls (FW) and Next-Gen Firewalls (NGFW)
- Unified threat management (UTM)
- Intrusion Detection Systems (IDS)

Cloud Security

- Cloud Access Security Brokers (CASB)
- Cloud Workload Protection Platforms (CWPP)

Threat Intelligence

- Cyber Threat Intelligence (CTI)

Identity Security

- Identity and Access Management (IAM)
- Privileged Access Management (PAM)

OT / IoT Security / Security Awareness

By transport type

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- File
- 1c-log and 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

By type of data

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

By vendor

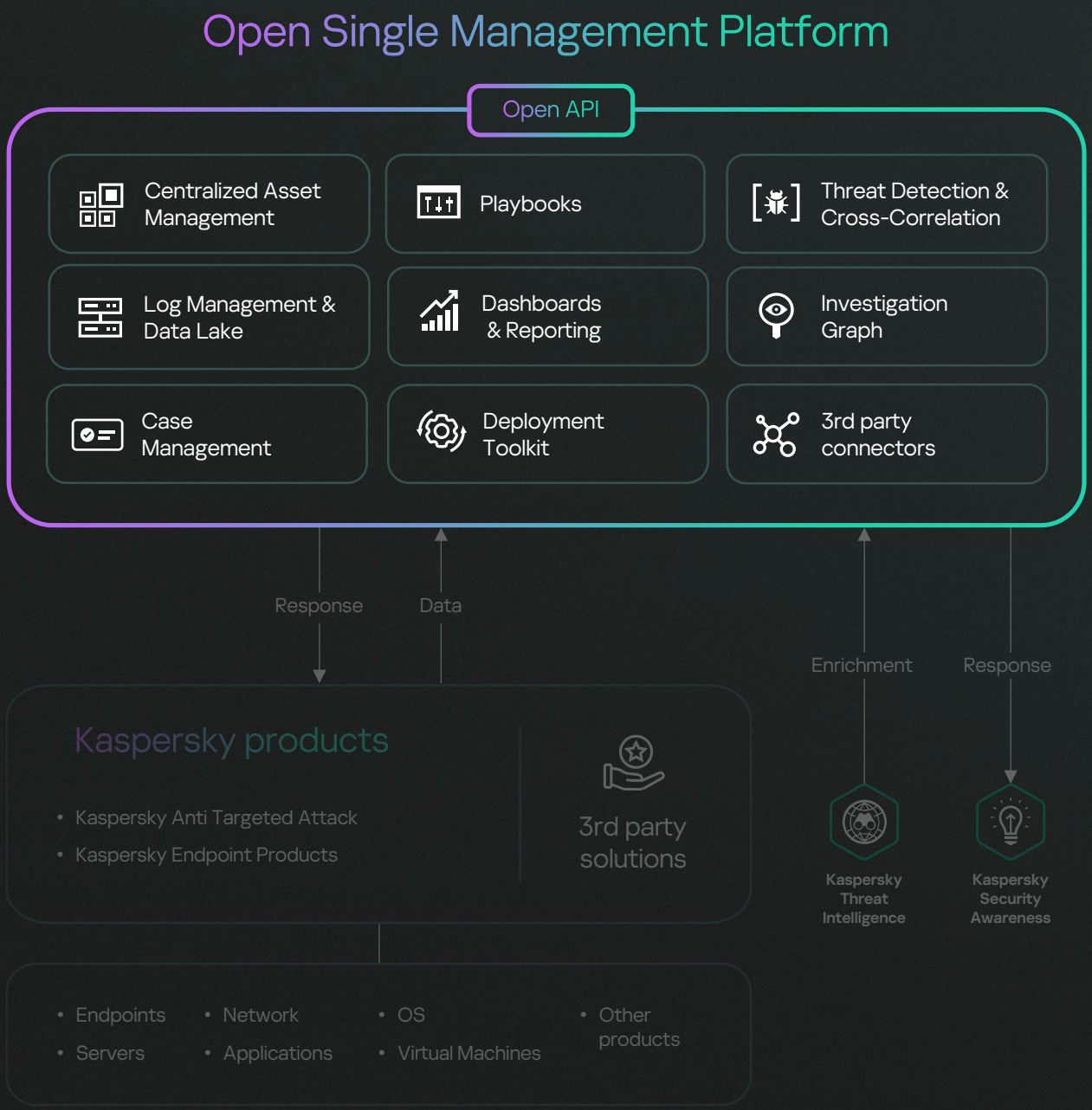
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard — Firebox
- Winchill Fracas
- Zettaset
- Zscaler & etc.

What we offer

Kaspersky XDR is available in two options.

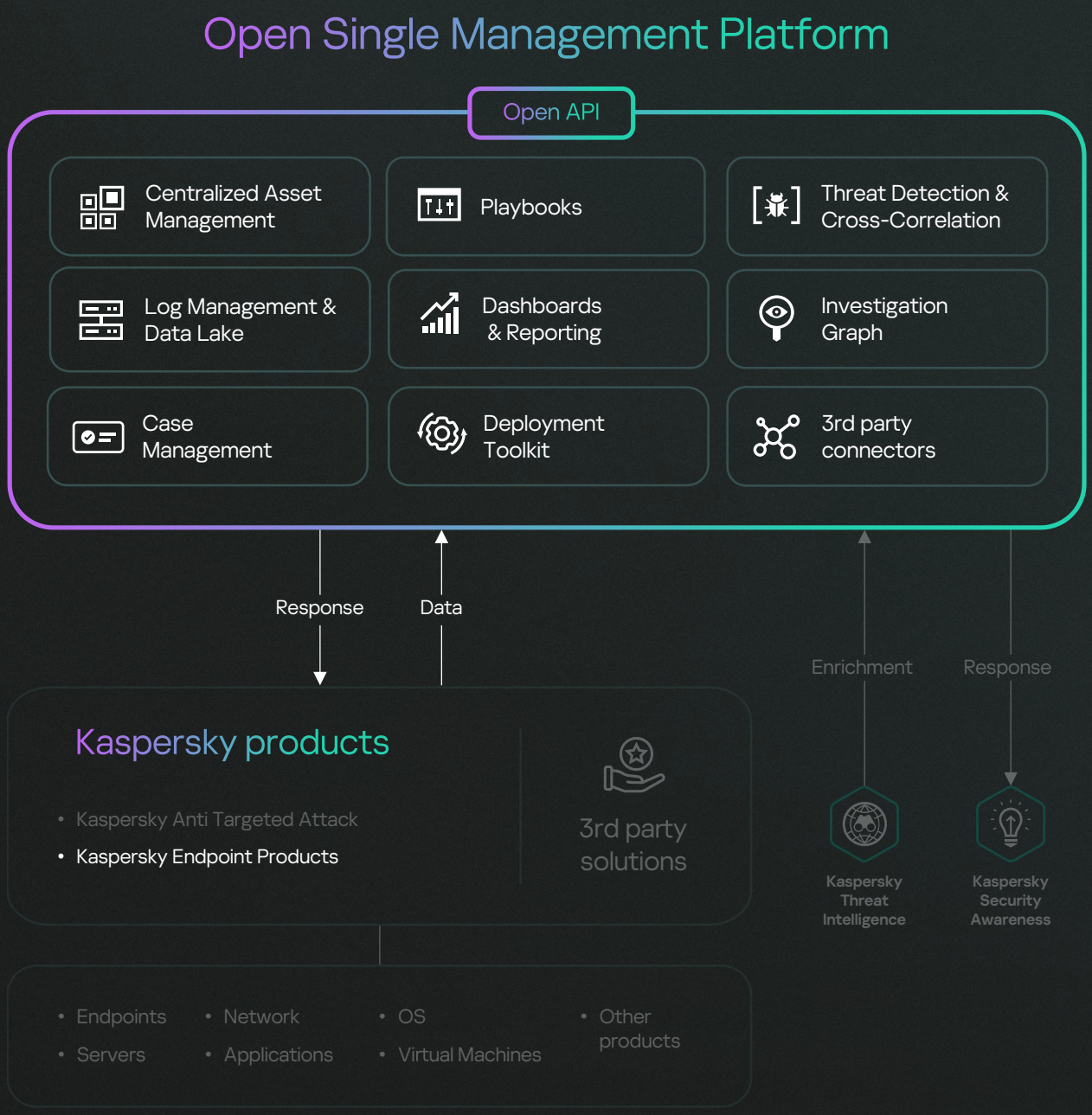
Kaspersky XDR Core

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



Kaspersky Next XDR Expert

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



Added value with supplementary sensors

Kaspersky XDR supports seamless integration of supplementary sensors designed to protect specific assets, integrating seamlessly into XDR to deliver an added layer of value, and transforming XDR into a cohesive platform that gives analysts a centralized workspace spanning all integrated solutions.

Kaspersky XDR not only boosts your defenses through EDR, but also offers flexible integration capabilities, so customers can add products to the ecosystem at any point.

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Open Single Management Platform and its components	Cross-correlation Engine • 3rd party connectors • Log Management & Data Lake • Threat Detection and Cross-correlation • Asset Management • Dashboards & Reporting	●	●
	XDR components • Case Management • Response automation and orchestration (playbooks) • Investigation • Deployment Toolkit • Open API	●	●
Kaspersky Endpoint functionality*	Automated, semi-automated & manual detection		●
	Monitoring across protected endpoints		●
	Threat containment		●
	Recovery options		●
	Mobile protection and management		●
	Cloud discovery and blocking		●
	Security for MS O365, data discovery		●
	Cybersecurity Training for IT administrator		●

* Feature availability varies depending on the implementation method

Kaspersky XDR Core

Kaspersky Unified Monitoring and Analysis Platform

XDR components

Kaspersky Next XDR Expert

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next EDR Foundations

Kaspersky Endpoint Detection and Response Expert

XDR components

Introducing Kaspersky Next

Kaspersky Next EDR Foundations

Robust security for everyone

Protect all your endpoints

If you need

- Strong endpoint protection
- Basic security controls
- Maximum automation

Kaspersky Next EDR Optimum

Build up your defenses

Boost your security with essential investigation and response

If you need

- Enhanced visibility and response capabilities
- Expanded cloud security
- Enterprise-grade controls

Kaspersky Next XDR Expert

Equip your experts

Protect your business against the most complex and advanced threats

If you need

- Advanced threat detection
- Seamless integration
- Powerful threat-hunting tools

Why Kaspersky XDR

Most tested. Most awarded. Kaspersky protection.

Kaspersky is an established global cybersecurity company with a strong track record of security expertise. We've been protecting organizations around the world for over 25 years and have received countless awards and accolades for our products and services. Between 2013 and 2022, Kaspersky products:

827

participated in 827 independent tests and reviews

587

achieved 587 first places

685

achieved top-three finishes

In 2023, Kaspersky was named the Leader in the XDR solutions market by leading global technology research and advisory firm ISG. ISG defines 'leaders' as having a comprehensive product and service offering and represent innovative strength and competitive stability.

Learn more

Kaspersky Extended Detection and Response

Request a Demo

www.kaspersky.com

#kaspersky
#bringonthefuture