Kaspersky Next XDR Expert

Ongeëvenaard inzicht. Totale beveiliging.

kaspersky

De complexiteit van cyberbeveiliging in bedrijven

Het cyberbedreigingslandschap is een enorme uitdaging voor organisaties om hun cyberbeveiliging bij te houden terwijl ze focussen op de kernactiviteiten. Gezien het toenemende aanvalsoppervlak, de wettelijke vereisten en de wereldwijde vaardigheidskloof, is het niet gek dat moderne bedrijven zo onder druk staan – en waarom zoveel cyberaanvallen slagen.

51%

van de bedrijven heeft moeite om met de huidige tools geavanceerde bedreigingen op te sporen en te onderzoeken

68%

van de bedrijven heeft eens te maken gehad met een gerichte aanval op hun netwerk met gegevensverlies als gevolg

$ 6 biljoen

per jaar: de jaarlijkse kosten van cybercriminaliteit wereldwijd

400000

nieuwe stukken malware worden dagelijks gedetecteerd

Bronnen: Kaspersky, PurpleSec en CybersecurityVentures

Kaspersky Extended Detection and Response

Volledige zichtbaarheid. Ongeëvenaarde bescherming.

Als onderdeel van de Kasperksy Next-productlijn hebben we Kaspersky Next XDR Expert geïntroduceerd, een oplossing waarin de Kaspersky XDR-aanpak wordt gebruikt en die een allesomvattend overzicht biedt van de beveiliging van een bedrijf.

Kaspersky XDR is een robuuste cyberbeveiligingsoplossing die bescherming biedt tegen geavanceerde cyberbedreigingen. Het biedt volledige zichtbaarheid, samenhang en automatisering, waarbij gebruik wordt gemaakt van diverse gegevensbronnen, waaronder endpoint-, netwerk- en cloudgegevens.

Het is van het Kaspersky Anti-Targeted Attack-platform als Native XDR in 2016 uitgegroeid tot Open XDR in 2023 en het biedt een allesomvattende kijk op beveiliging. Kaspersky XDR kan eenvoudig worden beheerd vanaf het Open Single Management Platform en het biedt een uitgebreide beveiliging op locatie, waarmee gevoelige gegevens van klanten binnen hun eigen infrastructuur blijven en aan de eisen voor datasoevereiniteit wordt voldaan.

Open XDR

Open XDR-oplossingen zijn ontwikkeld om te werken met een breed scala aan beveiligingsproducten, waardoor organisaties verschillende beveiligingsproducten van verschillende leveranciers kunnen samenvoegen, wat meer flexibiliteit en leveranciersonafhankelijke mogelijkheden biedt.

Native XDR

Native XDR-oplossingen werken doorgaans naadloos samen met het eigen ecosysteem van beveiligingstools van de leverancier, wat een meer verenigde en samenhangende ervaring biedt. Deze oplossingen zijn bewust gemaakt voor samenwerking en bieden diepgaande integratie, automatisering en gestroomlijnde workflows binnen de beveiligingsproductsets van de leverancier.

Belangrijkste technologieën

We bieden Open XDR aan als een enkel open platform , een universele tool om een verenigd ecosysteem van cyberbeveiligingsproducten te creëren. De kern van Kaspersky XDR wordt gevormd door onze toonaangevende oplossingen: het Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations en Kaspersky Endpoint Detection and Response. Voor geavanceerd netwerkbeheer is KATA een extra optie.

Bewaking en analyse

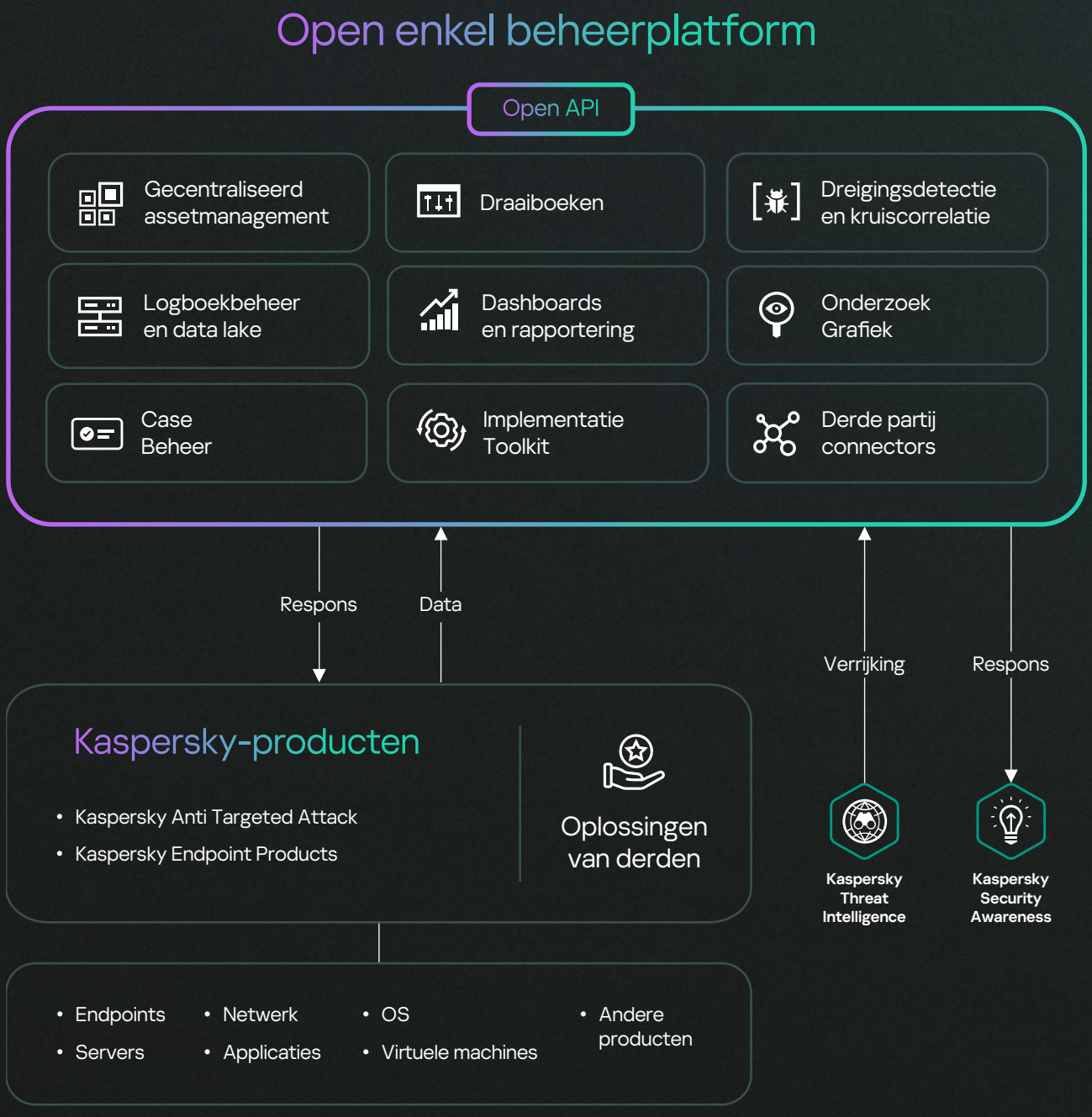
Biedt een gecentraliseerde verzameling en analyse van logs, samenhang van realtime beveiligingsgebeurtenissen en tijdige melding van incidenten. Bevat een kant-en-klare set van samenhangregels en toegang tot het uitgebreide aanbod van Kaspersky Threat Intelligence-services voor het identificeren en prioriteren van bedreigingen, aanvallen en IoCs.

Endpointbescherming

Biedt robuuste endpointbescherming, bescherming tegen ransomware, malware en bestandsloze aanvallen. Onze endpointbescherming, op locatie of in de cloud, maakt gebruikt van machine learning en gedragsanalyse om alle soorten endpoints met elk groot besturingssysteem te beschermen.

Endpoint Detection and Response

Levert uitgebreid overzicht en uitstekende verdediging voor alle endpoints van een organisatie. Betere opsporing en ontdekking van bedreigingen dankzij de unieke, uitgebreide informatie van Kaspersky over bedreigingen en automatisering van routinetaken, begeleide onderzoeksprocessen en aanpasbare detecties die een snellere oplossing van incidenten bevorderen.



Krachtige functies, aanzienlijke voordelen

Realtime gegevensfusie van derden

De mogelijkheid om gegevens uit bronnen van derden te integreren gaat verder dan alleen endpoints en wordt uitgebreid met realtime kruiscorrelatie.

Geautomatiseerde respons en herstel

Handmatige inspanningen en responstijd beperken door aangetaste endpoints af te zonderen of te isoleren, kwaadaardige activiteiten te blokkeren en kwetsbaarheden te herstellen.

Toonaangevende EPP/EDR

Kaspersky, dat wordt gezien als wereldleider, zet wereldwijd de standaard voor EPP/EDR-oplossingen. Kaspersky EDR blinkt wereldwijd uit, mede dankzij prijzen en actieve deelname aan internationale commissies zoals Interpol en MAPP.

Ongeëvenaarde schaalbaarheid

Kaspersky XDR kan de belasting van honderdduizenden endpoints op een enkele instantie ondersteunen en spoort bedreigingen zorgvuldig in realtime op terwijl een hoge beschikbaarheid wordt gewaarborgd.

Datasoevereiniteit

Kaspersky XDR is een van de weinige leveranciers die een uitgebreide XDR-oplossing op locatie biedt, die ervoor zorgt dat gevoelige gegevens van klanten binnen hun eigen infrastructuur blijft en dat aan de eisen voor gegevenssoevereiniteit wordt voldaan.

Naadloze en nauwe integratie met alle Kaspersky-producten

De interactie tussen producten bereikt een niveau dat buiten het bereik ligt van oplossingen van derden, met een uniform ondersteuningssysteem en naadloos geïntegreerd ontwerp.

Multi-tenancy die MSSP-scenario's mogelijk maakt

Bied XDR aan als een service met volwaardige tenants - gebruikers van de ene tenant kunnen de gegevens van andere tenants niet zien, terwijl de hoofdbeheerder (de MSSP) detectie- en responsprocessen voor alle klanten kan opzetten.

Geavanceerde aanpassing van beveiligingsscenario's en gegevensanalyse binnen de infrastructuur

Gebruikers kunnen complexe beveiligingsscenario's configureren met de extra mogelijkheid om gegevens over hun hele infrastructuur te analyseren.

Integratiemogelijkheden

Het breed scala aan integraties dat met Kaspersky XDR werkt, geeft een verenigd en gecontextualiseerd overzicht van mogelijke bedreigingen, waardoor je beveiligingsteam over alle tools en informatie beschikt die het nodig heeft om jouw organisatie te beschermen tegen alles wat cybercriminelen bij jou proberen.

De integratiemogelijkheden van het product omvatten de mogelijkheid om gegevens (logs) te ontvangen van andere systemen en apparaten en om automatische reacties in andere producten in te stellen. Kaspersky XDR wordt geleverd met een breed scala aan kant-en-klare integraties met producten van Kaspersky en van derden. Het is ook mogelijk om extra integraties toe te voegen die door hetzij Kaspersky Professional Services, hetzij partners of klanten zelf kunnen worden ontwikkeld (inclusief het gebruik van de API-mogelijkheden van koppelbare producten). Integratie is mogelijk met systemen uit verschillende domeinen en van verschillende leveranciers. Daarnaast worden talloze protocollen en indelingen voor gegevens ondersteund.

Per beveiligingsdomein

Endpoint Security

- EPP- en EDR-oplossingen

Netwerk-, web- en e-mailbeveiliging

- E-mailbescherming
- Netwerkdetectie en -respons (NDR)
- Firewalls (FW) en next-gen firewalls (NGFW)
- Unified threat management (UTM)
- Intrusion Detection Systems (IDS)

Cloudbeveiliging

- Cloud Access Security Brokers (CASB)
- Cloudworkloadbeschermings-platforms (CWPP)

Dreigingsinformatie

- Cyberbedreigingsinformatie (CTI)

Identiteitsbeveiliging

- Identiteits- en toegangsbeheer (IAM)
- Bevoorrecht toegangsbeheer (PAM)

OT / IoT-beveiliging / Beveiligingsbewustwording

Per transporttype

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

Per soort gegevens

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

Per leverancier

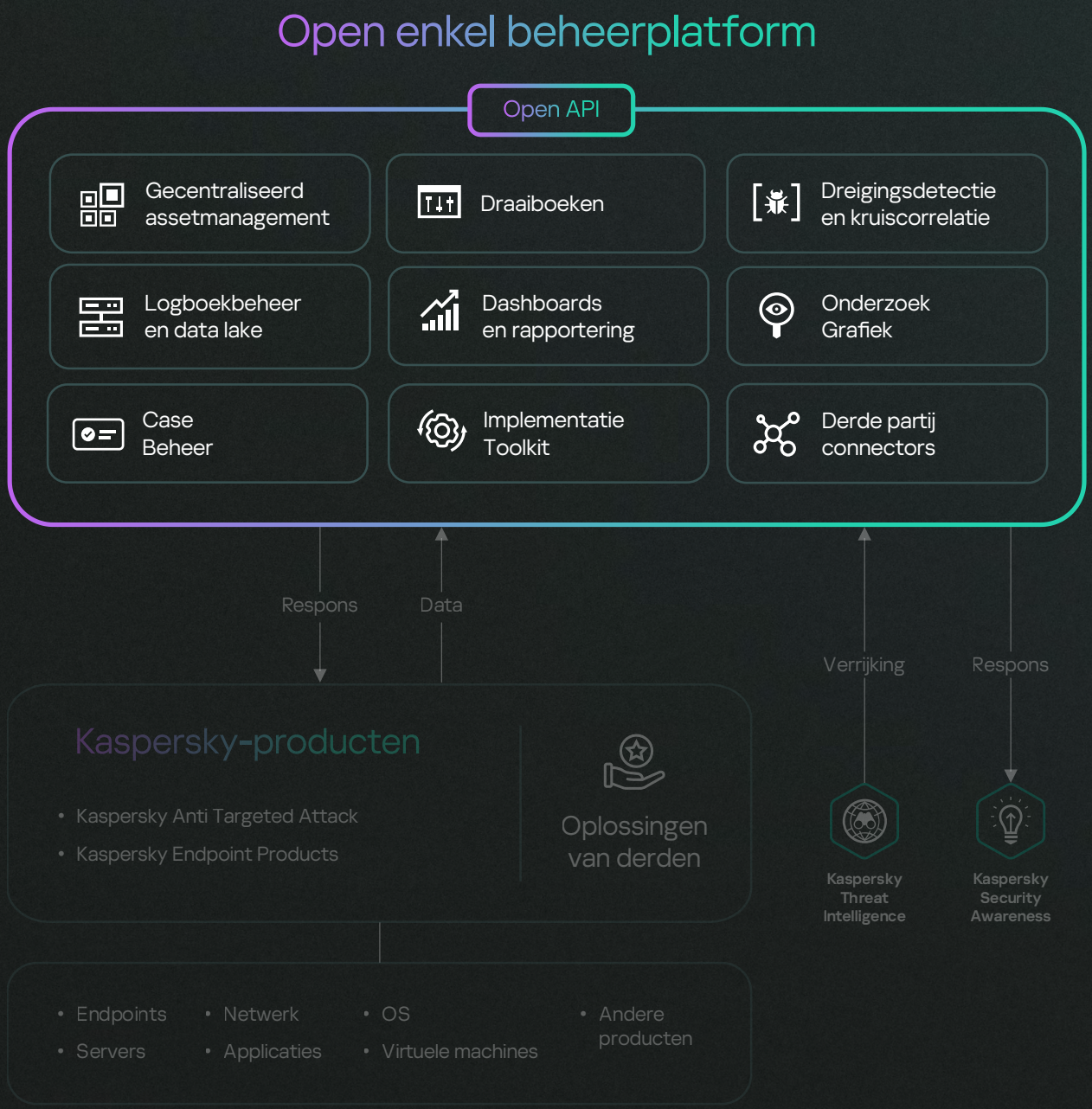
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- 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.

Wat hebben we te bieden?

Er zijn twee opties voor Kaspersky XDR beschikbaar.

Kaspersky XDR Core

Kaspersky XDR Core is voor klanten die al endpoint- en EDR-oplossingen hebben en deze niet willen vervangen, maar de functionaliteit willen uitbreiden met een correlatie-engine, geautomatiseerde reacties en connectors van derden.



Kaspersky Next XDR Expert

Kaspersky Next XDR Expert combineert de beste endpointbeveiliging met de geavanceerde detectiemogelijkheden van Kaspersky EDR Expert, een correlatie-engine en geautomatiseerde reacties. Connectors van derden kunnen worden toegevoegd om alle gegevens samen te voegen.

Toegevoegde waarde met aanvullende sensors

Kaspersky XDR ondersteunt naadloze integratie van aanvullende sensors die zijn ontworpen om specifieke middelen te beschermen, naadloos te integreren in XDR om toegevoegde waarde te leveren en XDR om te zetten in een samenhangend platform dat analisten een gecentraliseerde werkruimte biedt met alle geïntegreerde oplossingen.

Kaspersky XDR versterkt niet alleen je EDR-bescherming, maar biedt ook flexibele integratiemogelijkheden, zodat klanten op elk gewenst moment producten aan het ecosysteem kunnen toevoegen.

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Open enkel beheerplatform en zijn componenten	Kruiscorrelatie-engine • Connectors van derden • Logboekbeheer en data lake • Dreigingsdetectie en kruiscorrelatie • Assetmanagement • Dashboards en rapportering	●	●
	XDR-componenten • Casemanagement • Responsautomatisering en -uitvoering (draaiboeken) • Onderzoek • Implementatietoolkit • Open API	●	●
Functies van Kaspersky Endpoint*	Geautomatiseerde, semi-geautomatiseerde en handmatige detectie		●
	Bewaking van beschermde endpoints		●
	Indamming van dreiging		●
	Herstelopties		●
	Mobiele bescherming en beheer		●
	Cloud discovery en blocking		●
	Beveiliging voor MS O365, data discovery		●
	Cyberbeveiligingstraining voor IT-beheerders		●

* Toekomstige beschikbaarheid varieert afhankelijk van de implementatiemethode

Kaspersky XDR Core

Kaspersky Unified Monitoring and Analysis Platform

XDR-componenten

Kaspersky Next XDR Expert

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next EDR Foundations

Kaspersky Endpoint Detection and Response Expert

XDR-componenten

We introduceren Kaspersky Next

Kaspersky Next EDR Foundations

Krachtige beveiliging voor iedereen

Bescherm al je endpoints

Als je het volgende nodig hebt:

- Sterke endpointbescherming
- Basisbeveiliging
- Maximale automatisering

Kaspersky Next EDR Optimum

Versterk je beveiliging

Geef je beveiliging een boost met essentiële onderzoeken en antwoorden

Als je het volgende nodig hebt:

- Verbeterde zichtbaarheid en antwoordmogelijkheden
- Uitgebreidere cloudbeveiliging
- Beveiliging op bedrijfsniveau

Kaspersky Next XDR Expert

Voorzie uw experts

Bescherm je bedrijf tegen de meest complexe en geavanceerde bedreigingen

Als je het volgende nodig hebt:

- Geavanceerde bedreigingsdetectie
- Naadloze integratie
- Krachtige tools voor het opsporen van bedreigingen

Waarom Kaspersky XDR?

Het meest getest. Het meest bekroond. Beveiliging door Kaspersky.

Kaspersky is een gevestigd, wereldwijd cyberbeveiligingsbedrijf met een sterke staat van dienst betreft beveiligingsexpertise. We beschermen al meer dan 25 jaar organisaties over de hele wereld en we hebben vele prijzen en lofbetuigingen ontvangen voor onze producten en services. Tussen 2013 en 2022 hebben Kaspersky-producten:

827

deelgenomen aan 827 onafhankelijke tests en beoordelingen

587

587 eerste plaatsen behaald

685

de top drie behaald

In 2023 werd Kaspersky door het toonaangevende wereldwijde technologieonderzoeks- en adviesbureau ISG uitgeroepen tot Leider in de markt voor XDR-oplossingen. ISG definieert 'leiders' als bedrijven die een uitgebreid product- en service-aanbod hebben en innovatieve kracht en concurrentiestabiliteit vertegenwoordigen.

Meer informatie

Kaspersky Extended Detection and Response

Een demo aanvragen

www.kaspersky.nl

#kaspersky
#bringonthefuture