



# Kaspersky Next

Toekomstgerichte beveiliging

Redenen waarom  
beveiligingsoperaties lastiger  
zijn tegenwoordig:

41% van de organisaties  
schrijft het toe aan  
het snel veranderende  
bedreigingslandschap

40% schrijft het toe aan het  
grotere aanvalsoppervlak<sup>1</sup>

Kaspersky Next combineert robuuste endpoint-bescherming en controles met de transparantie en snelheid van EDR en de zichtbaarheid en krachtige tools van XDR. Hierdoor ontstaan er drie eenvoudige productniveaus. Kies de tools die je nu nodig hebt en stap eenvoudig over naar een andere tool als je er klaar voor bent.

## Waar je mee te maken hebt



### Ontwikkende aanvallen

Ransomware, malware en databreuken ontwikkelen zich continu. Er wordt gebruikgemaakt van complexe technieken om detectie te vermijden en je infrastructuur te infiltreren via Business Email Compromise, aanvallen op de toeleveringsketen en kwetsbaarheden.



### Groter aanvalsoppervlak

Werken op afstand, migreren naar de cloud en onderweg werken is geweldig. Maar zo ontstaan er een hoop nieuwe manieren voor hackers om een voet aan de grond te krijgen. Ook moeten er hierdoor veel meer controles worden toegepast.



### Beperkte bronnen

Het is nog nooit zo goedkoop geweest om een aanval te plegen, maar jezelf beschermen kost daarentegen veel bronnen. Je behoeften zijn waarschijnlijk groter dan je budget. Dit maakt TCO belangrijker dan ooit tevoren.



### Strengere regelgeving

GDPR, CCPA, PCI DSS en vereisten voor het vermelden van databreuken leggen nog meer druk op beveiligingsafdelingen als het gaat om beveiliging en rapportage.



### Groeiende complexiteit

IT- en cyberbeveiligingsinfrastructuren hebben niet de neiging om eenvoudiger en compact te worden. Ze groeien juist snel en ook worden er bij elke tool nieuwe servers, consoles en integraties toegevoegd om te behouden.



### Dus... Hoe staat het ervoor?

Specialisten op het gebied van cyberbeveiliging hebben veel aan hun hoofd door de grote hoeveelheid projecten, urgente taken, innovaties en eindeloze calls en meetings. Nieuwe tools en upgrades zouden je meer tijd moeten geven en niet ervoor zorgen dat je juist minder tijd hebt.

<sup>1</sup> SOC Modernization and the Role of XDR, Enterprise Strategy Group, 2022

51% van de huidige tools heeft moeite met het detecteren en onderzoeken van geavanceerde bedreigingen<sup>1</sup>



## Beveiligingsinnovatie

Kaspersky Next, dat is gebouwd op de basis van onze **bekroonde** endpointbeveiliging, voldoet aan al je behoeften en helpt je om snel en probleemloos EDR en XDR te gebruiken met weinig bronnen.

## Er is hulp beschikbaar

Kaspersky Next is de nieuwe productlijn van Kaspersky die je beveiliging versterkt met EDR en XDR en wordt ondersteund door sterke endpoint-bescherming. Het helpt om je aanvalsoppervlak te beveiligen en aanvallen te stoppen voordat ze schade kunnen veroorzaken.



## Op basis van machine learning

Onze producten maken gebruik van een reeks detectietechnologieën, waarvan machine learning een van de belangrijkste is. Het ondersteunt de effectieve detectie en het oplossen van complexe en nieuwe bedreigingen.



## De perfecte keuze voor jou

Er is geen algemene oplossing voor problemen op het gebied van cyberbeveiliging. Daarom heeft Kaspersky Next drie niveaus: de basis van endpoint-bescherming, het ontwikkelen van je expertise en het uitrusten van je experts met geavanceerde tools.

### Belangrijkste voordelen

- Bescherm je bedrijf tegen verschillende soorten bedreigingen en voorkom verliezen en verstoringen
- Kies het niveau dat het beste past bij je unieke behoeften
- Migreer eenvoudig van het ene niveau naar het andere naarmate je beveiligingsbehoeften toenemen en zich ontwikkelen
- Profiteer van EDR-functies op elk niveau op basis van je vereisten en bronnen
- Controleer je hele infrastructuur met uitgebreide open XDR
- Krijg ongeëvenaarde endpoint-bescherming op basis van machine learning op elk niveau
- Beheer je beveiliging via de cloud of lokaal
- Houd meer tijd over om te besteden aan andere belangrijke projecten dankzij automatiseringsfuncties voor gewone cyberbeveiligingstaken

## Beschermingsstructuur

Kaspersky Next biedt drie niveaus op basis van je meest kritieke cyberbeveiligingsbehoeften. Het is gemakkelijk om van niveau te wisselen naarmate je meer behoefte hebt aan cyberbeveiliging. Hierdoor worden je beveiligingsfuncties snel geüpgraded.



Aanbevolen gebruik  
IT-team houdt zich bezig met beveiliging

Toegevoegde waarde  
Garandeer bescherming van al je endpoints

Belangrijkste functies:

- Endpointbescherming
- Analyse van kernoorzaak
- Beveiliging en IT-beheer



Aanbevolen gebruik  
Klein cyberbeveiligingsteam

Toegevoegde waarde  
Geef je beveiliging een boost met eenvoudig onderzoek en respons

Belangrijkste functies:

- Geavanceerde endpointbescherming
- Cloudbescherming
- EDR-begeleiding en -automatisering



Aanbevolen gebruik  
Groot cyberbeveiligingsteam of SOC

Toegevoegde waarde  
Belangrijkste professionele tool voor je beveiligingsexperts

Belangrijkste functies:

- EDR met volledige functies
- IRP-workflow en verzameling van waarschuwingen
- ML en geavanceerde detectie

<sup>1</sup> SOC Modernization and the Role of XDR, Enterprise Strategy Group, 2022

69% van de aanvallen duurde gemiddeld slechts 2 dagen<sup>1</sup>

## Gebruiksscenario's

Kaspersky Next lost je kritieke cyberbeveiligingsproblemen op.



### Kaspersky Next EDR Foundations



#### Bescherm je endpoints

Met onze bekroonde endpoint-beschermingsengine ben je automatisch beschermd tegen malware, ransomware en andere belangrijke bedreigingen.



#### Krijg zichtbaarheid

Onderzoek bedreigingen met analyse van oorzaken en bepaal snel de omvang. Je hoeft niet meer te raden: ken je bedreigingen.



#### Verklein het aanvalsoppervlak

Gebruik controles voor apparaten, internet en applicaties en bescherm je mobiele apparaten om het aantal manieren te verkleinen waarop aanvallers in je systemen kunnen breken.



### Kaspersky Next EDR Optimum



#### Reageer snel

Reageer op aankomende ongrijpbare bedreigingen met één klik en maak eenvoudig een automatiseringstaak voor terugkomende aanvallen. Tijd om te reageren is een van de belangrijkste onderdelen van effectieve beveiliging.



#### Ontwikkel je expertise

Niet iedereen heeft meteen een complexe en krachtige EDR nodig, maar je moet ergens beginnen. Zichtbaarheid, analyse en respons in één pakket helpt je bij je EDR/XDR-traject.



#### Cloudbeveiliging

Ontdek, beperk en blokkeer toegang tot onder andere ongeautoriseerde cloudbronnen, diensten en berichtenapps. Krijg zichtbaarheid en controle over MS SharePoint Online, OneDrive en Teams.



### Kaspersky Next XDR Expert



#### Pak complexe bedreigingen aan

Wanneer je bedrijf het doelwit is van een geavanceerde of complexe aanval, moet je experts uitrusten met de meest krachtige tools en informatie die beschikbaar is. Verzameling, gegevensanalyse en geavanceerde detectie zijn essentieel.



#### Kruisasset-beveiliging

Door kruiscorrelatie uit te voeren voor gegevens van verschillende bronnen, deze te integreren met producten van externe partijen en routinetaken te automatiseren, kun je je experts in staat stellen om op zoek te gaan naar bedreigingen en erop te reageren op nauwkeurige, snelle en systematische wijze.



#### Draaiboeken

Automatisering en integratie van meerdere vooraf ingestelde draaiboeken verlaagt je Mean-Time-to-Respond drastisch en houdt zelfs geavanceerde bedreigingen tegen voordat ze effect kunnen hebben.

<sup>1</sup> Incident Response Analyst Report, Kaspersky, 2022

# Inhoud

Bekijk de specifieke belangrijke functies op elk niveau.



## Endpointbescherming

Bestand, web en e-mail, anti-virus, netwerkbescherming, AMSI, preventie van exploit, oplossing, gedragsdetectie, HIPS



## Beveiligingsbeheer

Firewall, web, apparaat, applicatiecontroles, bescherming en beheer van mobiele apparaten



## IT-scenario's

Beoordeling van kwetsbaarheden, patchbeheer, wissen van gegevens, SW/HW-voorraad, apps van externe partijen en installatie van besturingssystemen, verbinding op afstand



## Encryptie

Encryptie en encryptiebeheer



## Cloudbeveiliging

Cloud Discovery en blocking, beveiliging voor MS Office 365, Data Discovery



## Training

Cyberbeveiligingstraining voor IT-beheerders



## Essentiële EDR-mogelijkheden

Analyse van oorzaken, IoC-scan, endpoint-respons



## Geavanceerde EDR-mogelijkheden

Telemetrie verzamelen, bedreigingen opsporen, Indicator of Attack-detectie (IoA), MITRE ATT&CK in kaart brengen



## XDR-mogelijkheden

Verzameling van waarschuwingen, sandbox, AD-integratie, TI-verrijking, verbindingen van externe partijen, verbeterde onderzoekstools, inlogbeheer en gegevenslek, volledig geautomatiseerde respons, draaiboeken, detectie van bedreigingen en kruis-correlatie



	Pro-weergave	Cloud	Cloud	Niet van toepassing
<b>Beheerconsole</b>  Beschikbaar in de cloud of lokaal in twee weergaven:	Vereenvoudigd, gemakkelijk te beheren, maximaal aantal gebruikers: 2500			
	<b>Expert-weergave</b>  Gedetailleerd, aanpasbaar, minimaal aantal gebruikers voor cloud: 300	Cloud en lokaal	Cloud en lokaal	On-prem

Bekijk de bijbehorende Functielijst van het product voor de beschikbaarheid van specifieke functies in het type console dat je hebt gekozen.

<sup>1</sup> Beschikbare functies: Beoordeling van kwetsbaarheden, SW/HW-voorraad

<sup>2</sup> Beschikbare functies: Cloud Discovery

<sup>3</sup> Beschikbare functies: Analyse van oorzaken



43% van de organisaties noemt de kosten die zijn verbonden aan het beveiligen van steeds complexere technologische omgevingen als een van hun belangrijkste ITSec-uitdagingen<sup>1</sup>



## Overweeg beheerde beveiliging

Kaspersky Managed Detection and Response

- 24 uur per dag beheerde bescherming tegen ongreepbare bedreigingen
- Flexibiliteit die past bij elke sector en organisatorische behoefte
- Kosteneffectieve en volledig gerechtvaardigde investering in IT-beveiliging

# Til je beveiliging naar een hoger niveau

Externe expertise en aanvullende diensten kunnen je beveiliging naar een hoger niveau tillen.

Hier zijn enkele diensten die we aanraden en die je ervaring met Kaspersky Next verbeteren.



## Verspil geen tijd meer

Kaspersky Professional Services

- Vermijd verkeerde configuratie en verklein de invloed van implementatie
- Los beoordelingen, deployment, onderhoud en optimalisatie waar nodig
- Krijg hulp bij upgrades en migratie van Kaspersky-producten
- Essentiële servicepakketten en projecten op maat



## Krijg ondersteuning van experts

Kaspersky Premium Support

- Maximaliseer het rendement van je investeringen en vermijd de belasting van mogelijkheden
- Een directe telefoonlijn naar prioriteitsondersteuning
- Speciale technische experts van Kaspersky
- Uitgebreide beschikbaarheid bij kritieke problemen

## En nu?

Wat elk niveau van Kaspersky Next te bieden heeft:



**Kaspersky Next  
EDR Foundations**

De meest eenvoudige manier om robuuste cyberbeveiliging te creëren.

- Krachtige endpointbescherming op basis van ML
- Automatisch herstel
- Verschillende automatiseringsfuncties
- Flexibele beveiligingscontroles
- EDR-tools voor analyse van hoofdoorzaken

[Meer informatie](#)



**Kaspersky Next  
EDR Optimum**

Bouw je beveiliging op en wees bestand tegen ongreepbare bedreigingen.

- Essentiële EDR-functionaliteit biedt zichtbaarheid, analyse en respons
- Sterke endpointbescherming
- Verbeterde controles, patchbeheer en cloudbeveiliging
- Cyberbeveiligingstraining voor IT

[Meer informatie](#)



**Kaspersky Next  
XDR Expert**

Bescherm je bedrijf tegen de meest complexe en geavanceerde bedreigingen.

- Kan probleemloos worden geïntegreerd met je bestaande beveiligingsinfrastructuur
- Zichtbaarheid in realtime en uitgebreide inzichten in bedreigingen
- Geavanceerde bedreigingsdetectie
- Kruisasset-correlatie
- Geautomatiseerde respons

[Meer informatie](#)

<sup>1</sup> IT Security Economics 2022, Kaspersky, 2022

## Over ons

Kaspersky is een wereldwijd cyberbeveiligingsbedrijf met meer dan 250.000 zakelijke klanten over de hele wereld. We bouwen al 25 jaar tools en bieden diensten aan die onze klanten veilig houden met onze meest geteste, meest bekoonde technologieën. We staan voor transparantie en onafhankelijkheid.

### IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment

**belangrijke speler**



### AV-Test

Advanced Endpoint Protection: Ransomware Protection Test

**Volledige bescherming**



### Radicati Group

Advanced Persistent Threat (APT) Market Quadrant

**Topspeler**



### Info-Tech

Champion for Endpoint Protection in 2023



### G2

Best estimated ROI for Enterprise in the fall of 2023



## Laten we ze eens beter bekijken

Ga naar <https://go.kaspersky.com/next> voor meer informatie over hoe Kaspersky Next je kan helpen om je bedrijf te laten groeien in een beveiligde omgeving.

Ontdek meer over [Kaspersky Next](#)



**Kaspersky  
Next**



**Kaspersky Next  
EDR Foundations**

[Meer informatie](#)



**Kaspersky Next  
EDR Optimum**

[Meer informatie](#)



**Kaspersky Next  
XDR Expert**

[Meer informatie](#)

Nieuws over cyber bedreigingen: [securelist.com](https://securelist.com)  
Nieuws over IT-beveiliging: [business.kaspersky.com](https://business.kaspersky.com)  
IT Security for SMB: [kaspersky.com/business](https://kaspersky.com/business)  
IT Security for Enterprise: [kaspersky.com/enterprise](https://kaspersky.com/enterprise)

**kaspersky.nl**

© 2024 AO Kaspersky Lab.  
Geregistreerde handelsmerken en servicemerken zijn het eigendom van de respectieve eigenaars.

Meer informatie over Kaspersky Next is te vinden op:  
<https://go.kaspersky.com/next>

Kies het niveau dat het beste bij je past door een korte enquête in te vullen in onze interactieve tool:  
[https://go.kaspersky.com/Kaspersky\\_Next\\_Tool](https://go.kaspersky.com/Kaspersky_Next_Tool)

