Kaspersky Next EDR Optimum

Til je endpointbeveiliging naar een hoger niveau en pak ongrijpbare bedreigingen direct aan

kaspersky

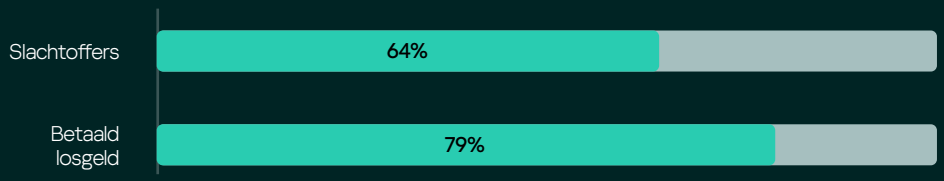
Kaspersky Next EDR Optimum

64% van de organisaties is al eens slachtoffer geworden van ransomware-aanvallen.

Hiervan heeft 79% losgeld betaald aan de aanvallers.

Hoe bedrijfsleiders omgaan met ransomware-aanvallen, Kaspersky, Mei 2022

Het is tijd om beveiliging naar een hoger niveau te tillen. Identificeer, analyseer en neutraliseer bedreigingen die zijn ontworpen om traditionele bescherming te omzeilen.



De uitdagingen

Bedreigingen omzeilen detectie

Ongrijpbare malware, ransomware, spyware en andere bedreigingen omzeilen traditionele detectie steeds beter doordat er legitieme systeemtools en andere geavanceerde technieken worden gebruikt tijdens aanvallen.

Ransomware-as-a-Service

Hackers kunnen tegenwoordig goedkope kant-en-klare tools kopen en iedereen aanvallen. Ze kunnen gegevens stelen, infrastructuur beschadigen en eisen om steeds grotere losgeldbedragen.

Beperkte bronnen

Infrastructuren worden steeds complexer en diverser, terwijl we bronnen (tijd, geld en mensen) te kort komen. Hierdoor blijft alles ongebruikt op de plank liggen.

"We stellen de uitgebreide oplossingen, betrouwbaarheid en snelle service en ondersteuning van Kaspersky op prijs. Ze verzekeren de beschikbaarheid van onze IT-omgeving."

Marcelo Mendes CISO, NEO

lees de casestudy

Hoe wij kunnen helpen

Kaspersky Next is onze belangrijkste productlijn en is ontworpen om je te helpen moeiteloos betere beveiliging op te bouwen. Of je nu op zoek bent naar essentiële EDR-functies of de weg baant voor toekomstig gebruik van XDR, de aanpasbare en robuuste cloud-eigen bescherming van Kaspersky Next, met een ongeëvenaarde ervaring op het gebied van cyberbeveiliging, is binnen handbereik.

Kaspersky Next EDR Optimum helpt je om ongrijpbare bedreigingen te identificeren, te analyseren en te neutraliseren met behulp van gebruiksvriendelijke geavanceerde detectie, vereenvoudigd onderzoek en mogelijkheden voor geautomatiseerde respons.

Geavanceerde bescherming

Onze geavanceerde detectiemechanismen bevatten gedragsanalyse en machine learning.

Dit wordt gecombineerd met eenvoudige visuele analysetools en snelle responsacties zodat je volledig inzicht krijgt in de bedreiging en bijbehorende omvang. Zo kun je de aanval stoppen voordat er schade wordt toegebracht.

Het verkleinen van het aanvalsoppervlak gebeurt op het endpoint en in de cloud met mogelijkheden voor cloudontdekking en blokkering, evenals met MS Office 365 Security.

Eén oplossing

Endpoint-beveiliging van de volgende generatie wordt gecombineerd met eenvoudige EDR voor verbeterde bescherming van laptops, werkstations, servers, cloud-workloads en virtuele omgevingen.

En slechts een enkele console om te implementeren en te beheren, in de cloud of lokaal.

Eenvoudig en efficiënt

We hebben Kaspersky Next EDR Optimum gebouwd met kleinere cyberbeveiligingsteams in gedachten. Dit is ideaal voor degenen die hun mogelijkheden voor incidentrespons willen upgraden en hun expertise willen ontwikkelen, maar die niet veel tijd hebben.

We automatiseren en optimaliseren de meeste taken, dus je besteedt alleen tijd aan belangrijke zaken. Daarnaast bieden we de training die jij en je IT-team nodig hebben om het meeste uit je nieuwe beveiligingsmogelijkheden te halen.

Nu kun je het volgende doen:

- **Cyberbedreigingen van tevoren** voorkomen
- **Je systemen en gegevens** beschermen tegen ongrijpbare bedreigingen
- **Huidige bedreigingen opmerken** voordat ze optreden
- **Ongrijpbare bedreigingen herkennen** op meerdere endpoints
- **Inzicht krijgen in de bedreiging** en deze snel analyseren
- **Schade voorkomen** dankzij snelle automatische respons
- **Tijd en bronnen besparen** dankzij een eenvoudige tool
- **Elk endpoint beschermen**: laptops, servers en cloud-workloads
- **Met een Pro-weergave** of Expert-weergaveconsole werken. Aan jou de keuze!

Nu heb je het volgende:

- **Endpointbeveiliging van de volgende generatie**
- **Mogelijkheden voor geavanceerde detectie** op basis van machine learning
- **Scannen op Indicator van compromis** (IoC)
- **Visueel onderzoek** en analysetools
- Alle nodige gegevens in een **enkele waarschuwingskaart**
- **Begeleiding en automatisering voor** ingebouwde respons
- **Enkele cloud- of lokale console** en automatisering
- Ondersteuning voor al je **werkstations, virtuele en fysieke servers, VDI-deployments en openbare cloud-workload**
- **Volledig productgetraind** IT-beveiligingspersoneel

Krijg de antwoorden op deze vragen op de belangrijkste momenten

Word ik aangevallen?

- **Pas geavanceerde detectie** op basis van machine learning toe
- **Download en scan IoC's** van securelist.com of andere bronnen om geavanceerde bedreigingen te vinden

Hoe is het gebeurd?

- Analyseer de bedreiging met behulp van een **visuele processtructuur**
- Krijg informatie over de acties via een **gedetailleerde grafiek**
- **Krijg inzicht in de oorzaken en de toegangspunten** in de infrastructuur

Hoe kan ik de bedreiging neutraliseren?

- **Gebruik meerdere responsopties:** isoleer de host, voorkom uitvoering van het bestand of verwijder het bestand
- **Scan andere hosts** op tekenen van de geanalyseerde bedreiging
- **Pas automatisch een respons toe** voor meerdere hosts bij ontdekking van een bedreiging (IoC)

Hoe zit het met andere bedreigingen?

- **Endpoint-beveiliging van de volgende generatie** is ontwikkeld om de meeste bedreigingen direct te kunnen tegenhouden
- **Verklein automatisch het aanvalsoppervlak** en pas je beleid aan
- **Beheer de applicaties en apparaten** die je gebruikers kunnen gebruiken

Hoe voorkom ik dit in de toekomst?

- **Maak gebruik van wat je hebt geleerd**: weet welke IP's en websites je moet blokkeren, welke beleidsregels je moet aanpassen en welke werknemers je moet trainen
- **Maak regels aan zodat je** zulke bedreigingen kunt voorkomen in de toekomst
- **Beveilig je cloud: ontdek, beperk en blokkeer toegang** tot onder andere ongeautoriseerde bronnen, diensten en berichtenapps op de cloud
- **Krijg zichtbaarheid en controle** over MS SharePoint Online, OneDrive en Teams

Hoe word ik hier beter in?

- **Gebruik de responsbegeleiding** in de waarschuwingskaart
- **Krijg toegang tot ons Threat Intelligence Portal** en de nieuwste TI
- **Ontwikkel je expertise** door bedreigingen te analyseren en erop te reageren
- **Haal voordeel uit ingebouwde training** en certificering, met interactieve oefeningen in een gesimuleerde omgeving

Hoe heb ik genoeg tijd voor alles?

- **Automatiseer beheer van kwetsbaarheden en patches**: de belangrijkste manieren om je endpoints veilig te houden
- **Beheer eigen encryptie** op afstand voor alle werknemers om bedrijfsgegevens veilig te houden
- **Automatiseer tijdrovende beheertaken** voor beveiliging en IT

Kaspersky Next EDR Optimum

Bouw je verdediging op
Geef je beveiliging een boost met essentieel onderzoek en respons

Als je het volgende nodig hebt:
- Verbeterde zichtbaarheid en antwoordmogelijkheden
- Uitgebreidere cloudbeveiliging
- Beveiliging op bedrijfsniveau

[1] Indicator van compromis

Kaspersky Next: jouw toekomstgerichte beveiliging

Kaspersky Next EDR Optimum is onderdeel van onze Kaspersky Next-productlijn. Het biedt robuuste endpointbescherming en controles door de transparantie en snelheid van EDR te combineren met de uitgebreide zichtbaarheid en krachtige toolset van XDR. Kaspersky Next EDR Optimum is verdeeld over drie productniveaus, 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.

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

Kaspersky Next EDR Optimum

Bouw je beveiliging op en wees bestand tegen ongrijpbare bedreigingen.

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

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

Waarom Kaspersky?

We zijn een wereldwijd privé-cyberbeveiligingsbedrijf met duizenden klanten en partners over de hele wereld. We staan voor transparantie en onafhankelijkheid. We bouwen al 25 jaar tools en bieden diensten om je veilig te houden met onze Meest geteste, Meest bekroonde technologieën.

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

Laten we ze eens beter bekijken

Ga naar https://go.kaspersky.com/next voor meer informatie over hoe Kaspersky Next EDR Optimum cyberbedreigingen aanpakt terwijl je beveiligingsteam wordt ondersteund en je bronnen worden bespaard.

Ontdek meer over Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations — Meer informatie

Kaspersky Next XDR Expert — Meer informatie

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

Nieuws over cyber bedreigingen: securelist.com
Nieuws over IT-beveiliging: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

kaspersky.nl