Wat is het verschil tussen een antivirus en een EDR-oplossing?

https://aucuba.nl/kennisbank/uncategorized/wat-is-het-verschil-tussen-een-antivirus-en-een-edr-oplossing/

Een antivirus en een EDR-oplossing beschermen beide endpoints, zoals laptops en servers, maar op een fundamenteel andere manier. Een antivirus herkent bekende bedreigingen op basis van een database met virushandtekeningen, terwijl **Endpoint Detection and Response** (EDR) verdacht gedrag in realtime analyseert en ook onbekende aanvallen kan detecteren en stoppen. Voor de meeste MKB-bedrijven is het verschil tussen deze twee beveiligingslagen bepalend voor hoe goed ze beschermd zijn tegen moderne cyberdreigingen. Dit artikel beantwoordt de meest gestelde vragen over antivirus, EDR en wanneer welke oplossing passend is.

Hoe werkt een traditionele antivirusoplossing?

Een traditionele antivirusoplossing werkt door bestanden en programma's te vergelijken met een database van bekende malware-handtekeningen. Wanneer een bestand overeenkomt met een bekende dreiging, blokkeert of verwijdert de antivirus het direct. Deze aanpak is effectief tegen veelvoorkomende, al langer bekende virussen en malware, maar heeft een duidelijke beperking: wat niet in de database staat, wordt niet herkend.

De werking van een antivirus steunt op drie kernprincipes. Ten eerste scant het software op bekende kenmerken van schadelijke code. Ten tweede controleert het bestanden bij het openen of downloaden, vaak in realtime. Ten derde worden de handtekeningdatabases regelmatig bijgewerkt door de leverancier, zodat nieuwe varianten van bekende virussen alsnog worden opgepikt.

Het nadeel van deze aanpak wordt steeds zichtbaarder naarmate cybercriminelen slimmer te werk gaan. Aanvallers passen hun code aan om detectie te omzeilen, gebruiken legitieme systeemtools voor kwaadaardige doeleinden of lanceren aanvallen die nergens op een handtekeningenlijst staan. Een antivirus is daartegen blind.

Wat is EDR en hoe verschilt het van antivirus?

EDR, voluit Endpoint Detection and Response, is een beveiligingsoplossing die continu het gedrag van processen, gebruikers en systemen op een apparaat monitort. In plaats van te vergelijken met bekende handtekeningen, analyseert EDR wat er op een endpoint *gebeurt* en grijpt in wanneer dat gedrag afwijkt van wat normaal is. Het verschil met antivirus zit in de diepgang, de snelheid van detectie en de mogelijkheid tot respons.

Waar een antivirus reageert op bekende bedreigingen, herkent EDR ook aanvallen die nog nooit eerder zijn gezien. EDR legt bovendien een gedetailleerd logboek bij van alle activiteiten op een apparaat, waardoor beveiligingsteams kunnen achterhalen hoe een aanval is verlopen en welke systemen zijn geraakt. Dat maakt onderzoek en herstel na een incident aanzienlijk eenvoudiger.

Samengevat zijn de belangrijkste verschillen:

- **Detectiemethode:** antivirus gebruikt handtekeningen, EDR analyseert gedrag
- **Reikwijdte:** antivirus blokkeert bekende malware, EDR detecteert ook geavanceerde en onbekende aanvallen
- **Respons:** antivirus verwijdert bestanden, EDR kan processen isoleren, aanvallen stoppen en forensisch onderzoek ondersteunen
- **Zichtbaarheid:** antivirus geeft beperkt inzicht, EDR biedt een volledig overzicht van wat er op een endpoint gebeurt

Welke bedreigingen mist een antivirus die EDR wel detecteert?

Een antivirus mist bedreigingen die geen bekende handtekening hebben of die gebruikmaken van legitieme systeemfuncties. EDR detecteert deze aanvallen wel, omdat het kijkt naar gedrag in plaats van naar de vorm van een bestand. Dit maakt EDR bijzonder effectief tegen een groeiende categorie van geavanceerde aanvallen.

Concrete voorbeelden van bedreigingen die een antivirus doorgaans niet oppikt:

- **Fileless malware:** aanvallen die volledig in het geheugen draaien en geen bestanden op schijf achterlaten
- **Zero-day exploits:** kwetsbaarheden die nog niet bekend zijn bij antivirusleveranciers
- **Living-off-the-land aanvallen:** aanvallers die legitieme tools zoals PowerShell of Windows Management Instrumentation misbruiken

- **Laterale beweging:** wanneer een aanvaller zich na een initiële inbraak door het netwerk verspreidt
- **Ransomware-varianten:** nieuwe of aangepaste versies die nog niet in handtekeningdatabases staan

Voor MKB-bedrijven is dit relevant omdat aanvallers steeds vaker juist deze technieken inzetten, wetende dat veel kleinere organisaties alleen op traditionele antivirussoftware vertrouwen.

Wanneer is een antivirus voldoende en wanneer heb je EDR nodig?

Een antivirus is voldoende voor thuisgebruikers of organisaties met een zeer laag risicoprofiel, minimale gevoelige data en beperkte digitale afhankelijkheid. Voor vrijwel elk MKB-bedrijf dat met klantgegevens, financiële informatie of bedrijfskritische systemen werkt, biedt een antivirus alleen onvoldoende bescherming in 2026.

EDR is aan te raden wanneer een of meer van de volgende situaties van toepassing zijn:

- Het bedrijf verwerkt persoonsgegevens of gevoelige klantinformatie
- Medewerkers werken op afstand of via onbeveiligde netwerken
- De organisatie is afhankelijk van digitale systemen voor haar dagelijkse bedrijfsvoering
- Er is geen intern IT-team dat actief beveiligingsincidenten monitort
- De sector heeft te maken met verhoogde cyberdreigingen, zoals zorg, juridische dienstverlening of financiën

De praktijk wijst uit dat ransomware-aanvallen en datalekken steeds vaker MKB-bedrijven treffen, juist omdat aanvallers weten dat de beveiliging daar doorgaans minder volwassen is. EDR verkleint dat risico aanzienlijk.

Wat kost een EDR-oplossing vergeleken met een antivirus?

Een EDR-oplossing is doorgaans duurder dan een traditionele antivirus, maar de kostenverschillen zijn genuanceerder dan alleen de licentieprijs. Bij het vergelijken van de totale kosten spelen meerdere factoren een rol die de uiteindelijke investering bepalen.

Factoren die de kosten van een EDR-oplossing beïnvloeden:

- **Aantal endpoints:** licenties worden vaak per apparaat of per gebruiker berekend

- **Beheerbehoefte:** EDR vereist actieve monitoring en opvolging, wat intern capaciteit vraagt of uitbesteed moet worden aan een partner
- **Integratie:** hoe goed de oplossing aansluit op bestaande systemen bepaalt de implementatiekosten
- **Serviceniveau:** sommige EDR-oplossingen worden geleverd als beheerde dienst, waarbij een partner de monitoring en respons overneemt

Tegenover de hogere investering staat een aanzienlijk lager risico op de kosten van een beveiligingsincident, zoals downtime, herstelwerkzaamheden, reputatieschade of boetes bij een datalek. Vanuit dat perspectief is EDR voor veel MKB-bedrijven een kosteneffectieve keuze.

Kan een bedrijf antivirus en EDR tegelijk gebruiken?

Ja, antivirus en EDR kunnen naast elkaar worden gebruikt, en in veel gevallen is dat zelfs de aanbevolen aanpak. Moderne EDR-oplossingen bevatten vaak al antivirusfunctionaliteit, maar sommige organisaties kiezen bewust voor een combinatie van beide als extra beveiligingslaag. Het is wel belangrijk dat de twee oplossingen goed op elkaar zijn afgestemd om conflicten of prestatieproblemen te voorkomen.

Wanneer beide oplossingen worden ingezet, dekt antivirus de basislaag af door bekende bedreigingen snel te blokkeren, terwijl EDR de diepere gedragsanalyse en incidentrespons verzorgt. Dit geeft organisaties zowel breedte als diepte in hun beveiliging.

In de praktijk adviseren wij MKB-bedrijven om te kiezen voor een geïntegreerde oplossing waarbij antivirus en EDR vanuit één platform worden beheerd. Dat vereenvoudigt het beheer, vermindert blinde vlekken en zorgt voor een consistente beveiligingsstrategie. Wil je weten welke combinatie het beste past bij jouw organisatie? Neem dan gerust contact met ons op voor een vrijblijvend adviesgesprek.