GIDS

De complete gids voor Endpoint Detection & Response

Werking, kosten, selectiecriteria, NIS2-verplichtingen en het verschil tussen EDR, XDR en MDR. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Endpoint Detection & Response is in korte tijd uitgegroeid van enterprise-luxe tot MKB-noodzaak. De cijfers spreken voor zich.

93%
van cyberverzekeringen eist bewijs van endpoint detection als acceptatie-eis
Diverse verzekeraarsbronnen [1]

70%
van serieuze malware in 2024 bestond uit fileless attacks -- onzichtbaar voor traditionele antivirus
Expert Insights 2025 [2]

273%
ROI over 3 jaar bij EDR-implementatie, terugverdientijd onder 6 maanden
Forrester TEI Study 2025 [3]

EUR 270K
gemiddelde schade per cyberincident voor MKB in Nederland
Hallo.eu / Cybercrimebeeld NL [4]

277 dagen
gemiddelde detectietijd zonder EDR -- met EDR: uren in plaats van maanden
BrightDefense / Industry data [5]

60%
van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige cyberaanval
Diverse bronnen [6]

24–27%
jaarlijkse groei van de wereldwijde EDR-markt (CAGR)
Mordor Intelligence / Grand View Research [7]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- endpoint monitoring als zorgplicht
Digitale Overheid [8]

1. Wat is EDR?

Endpoint Detection & Response (EDR) is beveiligingssoftware die endpoints -- laptops, desktops, servers en mobiele apparaten -- continu monitort op verdacht gedrag en automatisch reageert op dreigingen.

Het verschil met traditionele antivirus is fundamenteel. Antivirus werkt op basis van bekende signatures: het herkent malware die al eerder is gezien. EDR kijkt naar gedrag. Het analyseert procesactiviteit, bestandsinteracties en gebruikerspatronen om ook onbekende dreigingen te detecteren -- inclusief fileless attacks, zero-day exploits en geavanceerde ransomware.

KERNFUNCTIES

FUNCTIE	WAT HET DOET
Continue monitoring	Real-time registratie van alle endpoint-activiteit, 24/7
Gedragsanalyse	Detectie op basis van afwijkend gedrag, niet alleen bekende signatures
Geautomatiseerde respons	Automatisch isoleren van besmette endpoints voordat schade zich verspreidt
Forensisch onderzoek	Tijdlijn van het aanvalsverloop voor root cause analysis
Threat hunting	Proactief zoeken naar verborgen dreigingen die nog niet actief zijn
Threat intelligence	Correlatie met actuele dreigingsdatabases wereldwijd

> **In een zin:** Traditionele antivirus is een slotgracht die bekende vijanden buitenhoudt. EDR is een bewakingssysteem dat verdacht gedrag detecteert, automatisch ingrijpt en een volledig verslag levert van wat er is gebeurd.

2. Waarom is het belangrijk?

Traditionele antivirus beschermt nog steeds tegen bekende malware, maar dekt de moderne dreigingsrealiteit niet meer. De redenen om over te stappen naar EDR zijn concreet en meetbaar.

CYBERVERZEKERINGEN EISEN HET

93% van alle actieve cyberverzekeringen in 2025 vereist bewijs van endpoint detection, immutable backups en MFA-implementatie [1]. Zonder EDR krijg je geen cyberverzekering, of betaal je fors hogere premies. Voor MKB-bedrijven die een cyberverzekering willen afsluiten is EDR daarmee geen keuze meer -- het is een harde eis.

RANSOMWARE BESCHERMING

EDR detecteert ransomware via AI-gebaseerde gedragsanalyse met een detectiepercentage van 89% in 2025 [2]. Traditionele antivirus mist de meeste geavanceerde ransomware-varianten omdat ze geen bekende signature hebben. Bij een gemiddelde ransomware-schade van EUR 35.000 voor Nederlands MKB [9] is dat een risico dat je niet kunt veroorloven.

FILELESS ATTACKS DOMINEREN

Eind 2024 bestond circa 70% van alle serieuze malware uit fileless attacks [2] -- aanvallen die geen bestanden op de schijf plaatsen en daarmee onzichtbaar zijn voor traditionele antivirus. EDR detecteert deze aanvallen door procesgedrag te analyseren in plaats van bestanden te scannen.

DETECTIETIJD: MAANDEN VS UREN

SITUATIE	GEMIDDELDE DETECTIETIJD	IMPACT
Zonder EDR	277 dagen [5]	Aanvaller heeft maandenlang vrij spel
Met EDR	Uren -- 28% detecteert binnen enkele uren [5]	Schade beperkt tot minimum
Met AI-driven EDR	63% reductie in dwell time [5]	Aanval gestopt voordat laterale beweging plaatsvindt

REKENSOM

EDR kost EUR 30--185 per endpoint per jaar. Een gemiddeld cyberincident kost EUR 270.000 [4]. Bij 100 endpoints betaal je EUR 3.000--18.500 per jaar -- minder dan 7% van de potentiele schade van een enkel incident.

3. Hoe werkt het?

EDR draait op een lichtgewicht software-agent die op elk endpoint wordt geinstalleerd. Hieronder de technische werking in begrijpelijke taal.

AGENT-BASED DETECTIE

Op elk endpoint (laptop, desktop, server) wordt een kleine software-agent geinstalleerd. Deze agent draait op de achtergrond en registreert continu alle activiteit: welke processen draaien, welke bestanden worden geopend, welke netwerkverbindingen worden gemaakt en welke gebruikersacties plaatsvinden. Al deze data wordt naar een centraal dashboard gestuurd.

BEHAVIORAL ANALYSIS

In plaats van te zoeken naar bekende malware-signatures analyseert EDR gedragspatronen. Als een proces plotseling bestanden begint te encrypteren (ransomware-gedrag), ongebruikelijke netwerkverbindingen maakt (command & control), of probeert beveiligingstools uit te schakelen -- dan slaat EDR alarm, ook als de malware nooit eerder is gezien.

AUTOMATED RESPONSE

Bij detectie van een dreiging kan EDR automatisch ingrijpen:

- **Endpoint isolatie** -- het besmette apparaat wordt direct losgekoppeld van het netwerk, maar blijft bereikbaar voor onderzoek
- **Proces blokkering** -- het kwaadaardige proces wordt gestopt
- **Bestandsquarantaine** -- verdachte bestanden worden geisoleerd
- **Rollback** -- sommige EDR-oplossingen kunnen versleutelde bestanden herstellen naar de staat voor de aanval

FORENSISCH ONDERZOEK

EDR legt een volledige tijdlijn vast van elk incident: wanneer de aanval begon, welke stappen de aanvaller nam, welke systemen zijn geraakt en hoe de aanval zich verspreidde. Dit is essentieel voor de NIS2-meldplicht (24 uur) en voor het voorkomen van herhaling.

IMPLEMENTATIE IN DE PRAKTIJK

- **Fase 1 (1--2 weken):** Inventarisatie endpoints en risicobeoordeling
- **Fase 2 (2--4 weken):** Pilot op 10--20% van endpoints in Detect Only modus
- **Fase 3 (2--4 weken):** Tuning -- reduceren false positives, exceptions configureren
- **Fase 4 (2--6 weken):** Volledige uitrol over alle endpoints
- **Doorlopend:** Monitoring, policy reviews, threat hunting

4. Wat kost het?

EDR-kosten varieren van EUR 2 per endpoint per maand voor basisoplossingen tot EUR 50+ voor volledig managed services. De juiste keuze hangt af van je budget, teamgrootte en risiconiveau.

PRIJSOVERZICHT PER SEGMENT

SEGMENT	PRIJS/ENDPOINT/ MAAND	PRIJS/ENDPOINT/ JAAR	TYPISCHE FEATURES
Basis EDR	EUR 2--5	EUR 24--60	Next-gen antivirus + basisdetectie
Standaard EDR	EUR 5--12	EUR 60--144	Volledige EDR + automatische respons
Premium EDR	EUR 12--18	EUR 144--216	+ Threat hunting + forensics + threat intelligence
EDR + MDR	EUR 15--50+	EUR 180--600+	+ 24/7 managed service door extern SOC-team

MKB INDICATIES (JAARKOSTEN)

ORGANISATIEGROOTTE	BASIS	STANDAARD	PREMIUM	MANAGED (MDR)
25 endpoints	EUR 600--1.500	EUR 1.500--3.600	EUR 3.600--5.400	EUR 4.500--15.000
50 endpoints	EUR 1.200--3.000	EUR 3.000--7.200	EUR 7.200--10.800	EUR 9.000--30.000
100 endpoints	EUR 2.400--6.000	EUR 6.000--14.400	EUR 14.400--21.600	EUR 18.000--60.000
250 endpoints	EUR 6.000--15.000	EUR 15.000--36.000	EUR 36.000--54.000	EUR 45.000--150.000

Volumekortingen gelden bij 50+, 100+, 500+ en 1.000+ endpoints. Mid-market onderhandeling levert typisch 15--25% korting op [10].

VERBORGEN KOSTEN

Let op kosten die niet in de licentieprijs zitten: premium support (EUR 15--20/endpoint/jaar extra), MDR add-ons die de kosten verdubbelen, eenmalige implementatiekosten en -- het belangrijkste -- de personeelskosten om alerts te verwerken. EDR zonder gekwalificeerd personeel is een dashboard zonder waarde [10].

5. Waar moet je op letten?

De EDR-markt is groot en onoverzichtelijk. Hieronder de selectiecriteria die je helpen een onderbouwde keuze te maken, zonder je te laten leiden door merknamen.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
Autonomie niveau	Kan de oplossing zelfstandig detecteren en reageren, of is handmatige interventie nodig? Hogere autonomie = minder personeel vereist.
MITRE ATT&CK scores	Onafhankelijke benchmark voor detectiecapabiliteit. Kijk naar het percentage gedetecteerde aanvalsstappen in recente evaluaties.
OS-support	Ondersteunt de oplossing alle besturingssystemen in je omgeving? Windows, macOS en Linux-support varieert sterk per leverancier.
Cloud-native architectuur	Cloud-native oplossingen zijn sneller te deployen, schalen beter en vereisen minder on-premise infrastructuur.
Managed vs self-managed	Zonder eigen SOC-team heb je managed EDR (MDR) nodig. Kies een leverancier die past bij je personeelssituatie.
Integraties	Koppeling met je SIEM, firewall, identity management en e-mailbeveiliging. Geisoleerde EDR mist context.
Rollback-capaciteit	Kan de oplossing door ransomware versleutelde bestanden terugzetten naar hun oorspronkelijke staat?
False positive ratio	46% van alle security-alerts blijkt false positive [11]. Een hoog percentage leidt tot alert fatigue.
Systeembelasting	Hoe zwaar is de agent? Bij oudere hardware of resource-beperkte endpoints is een lichtgewicht agent essentieel.
Exit-strategie	Hoe makkelijk en duur is het om over te stappen naar een andere leverancier? Evalueer dit bij selectie, niet bij vertrek.

10 VRAGEN AAN EEN LEVERANCIER

1. Wat is jullie detectiepercentage in de meest recente MITRE ATT&CK evaluatie?
2. Welke besturingssystemen worden volledig ondersteund (inclusief Linux-distributies)?

3. Kan de oplossing autonoom reageren zonder menselijke interventie?
4. Bieden jullie rollback-functionaliteit bij ransomware-aanvallen?
5. Wat is de gemiddelde systeembelasting van de agent op een standaard endpoint?
6. Hoe integreren jullie met onze bestaande security-stack?
7. Bieden jullie managed EDR (MDR) als add-on of apart product?
8. Wat is de gemiddelde opstarttijd en hoe verloopt de pilotfase?
9. Welke rapportages leveren jullie voor NIS2-compliance?
10. Wat zijn de contractvoorwaarden, volumekortingen en exit-kosten?

6. Veelgemaakte fouten

EDR is krachtig, maar verkeerde implementatie kan het onbruikbaar maken -- of erger, een vals gevoel van veiligheid creëren.

#	FOUT	GEVOLG	OPLOSSING
1	**Alert fatigue**	Gemiddeld 2.992 alerts per dag per organisatie [11]. 42--63% wordt nooit onderzocht. Echte dreigingen worden gemist.	Kies EDR met AI-triage of ga voor managed EDR (MDR)
2	**Onvolledige deployment**	Onbewaakte endpoints zijn vaak het startpunt van een aanval. Shadow IT en BYOD blijven blinde vlekken [12].	Verplichte installatie + asset discovery koppelen aan EDR-dashboard
3	**Direct in block-modus**	Kritieke bedrijfsapplicaties stoppen met werken. Productiviteitsverlies en weerstand bij gebruikers.	Start altijd in Detect Only modus. Test minimaal 2--4 weken voor je blokkeert.
4	**Set-and-forget**	EDR zonder continu tunen en updaten veroudert snel. Nieuwe aanvalstechnieken worden gemist [12].	Maandelijkse EDR-reviews, vendor-advisories volgen
5	**Te complexe policies**	Te veel verschillende beleidsregels per systeemtype wordt onbeheersbaar en leidt tot gaten [12].	Houd policies simpel en uniform. Minimaliseer uitzonderingen.
6	**Geen personeel voor monitoring**	EDR-alerts worden genegeerd. Twee derde van cybersecurity-professionals ervaart burnout [11].	Kies voor managed EDR (MDR) als je geen eigen SOC hebt

VUISTREGEL

Heb je minder dan 3 security-specialisten in dienst? Kies voor managed EDR (MDR). De kosten zijn hoger, maar de alternatiefkosten van gemiste alerts zijn dat ook. EDR zonder capaciteit om alerts te verwerken is gevaarlijk [13].

7. NIS2: endpoint vereisten

De Cyberbeveiligingswet (NIS2) noemt geen specifieke technologieen, maar stelt eisen die EDR direct adresseren. In de praktijk is endpoint detection een noodzakelijke bouwsteen voor compliance.

RELEVANTE VERPLICHTINGEN

NIS2-VEREISTE	HOE EDR HIERAAN BIJDRAAGT
Risicobeheersmaatregelen (Art. 21)	EDR biedt continue monitoring en detectie van dreigingen op alle endpoints
Incidentafhandeling	EDR automatiseert detectie, isolatie en forensisch onderzoek
Meldplicht (24 uur)	EDR levert de tijdlijn en details die nodig zijn voor snelle melding bij CSIRT [8]
Bedrijfscontinuiteit	EDR beperkt impact door snelle containment en isolatie
Toeleveringsketen-beveiliging	EDR beschermt endpoints die verbonden zijn met leverancierssystemen
Beveiligingstests	EDR-data ondersteunt vulnerability assessments en audits

> **Belangrijk:** EDR is geen expliciete NIS2-verplichting, maar wordt door vrijwel alle security-experts beschouwd als een noodzakelijke bouwsteen om aan de zorgplicht te voldoen. Het NCSC noemt endpoint detection als onderdeel van passende technische maatregelen [14].

MELDPLICHT EN EDR

De NIS2-meldplicht vereist:

- **Binnen 24 uur:** Early alert aan CSIRT met eerste beoordeling
- **Binnen 72 uur:** Incident notification met ernst, impact en scope
- **Binnen 1 maand:** Eindverslag met root cause analysis

Zonder EDR kun je deze tijdlijnen niet halen. EDR levert de forensische data die je nodig hebt om aan de meldplicht te voldoen [14].

8. EDR vs XDR vs MDR

De afkortingen lijken op elkaar, maar de verschillen zijn wezenlijk. Hieronder een heldere vergelijking om de juiste keuze te maken.

ASPECT	EDR	XDR	MDR
Type	Technologie (product)	Technologie (platform)	Service (uitbesteding)
Scope	Alleen endpoints	Endpoints + netwerk + cloud + e-mail + identiteit	Afhankelijk van onderliggende tech
Correlatie	Beperkt tot endpoint-events	Cross-layer correlatie	Door menselijke analisten + technologie
Wie beheert	Eigen IT-team	Eigen IT/security-team	Extern SOC-team (24/7)
Personeel nodig	Min. 1 security-specialist	1--2 security-specialisten	Geen intern security-personeel nodig
Investering	EUR 30--185/endpoint/jaar	EUR 80--250/endpoint/jaar	EUR 120--600/endpoint/jaar
Geschikt voor	Organisaties met eigen security-team	Complexe omgevingen met meerdere tools	MKB zonder eigen SOC

WANNEER KIES JE WAT?

- **Geen eigen security-team?** MDR is vrijwel verplicht [13]
- **Kleiner dan 50 medewerkers?** Managed EDR via een IT-partner
- **Eigen IT maar geen SOC?** MDR of co-managed EDR
- **Eigen SOC (5+ analisten)?** Self-managed EDR of XDR mogelijk
- **NIS2-plichtig zonder security-expertise?** MDR + compliance rapportage

9. Trends 2025--2026

De EDR-markt verandert snel. Hieronder de drie trends die bepalen hoe endpoint security er in 2026 uitziet.

AI-NATIVE ENDPOINT SECURITY

De industrie verschuift van statische playbooks naar AI-agents die zelfstandig kunnen redeneren, onderzoeken en handelen binnen expliciete guardrails. AI-driven EDR bereikt een 63% reductie in dwell time [5]. De verwachting is een halvering van de gemiddelde dwell time -- van 21 dagen naar circa 10 -- tegen eind 2026. Signature-loze detectie op basis van AI/ML wordt de standaard voor zero-day threats.

CLOUD WORKLOAD PROTECTION

EDR breidt uit van traditionele endpoints naar cloud workloads: virtuele machines, containers en Kubernetes-omgevingen. Lichtgewicht agents met lage overhead bieden real-time zichtbaarheid in cloud-native architecturen. Voor MKB-bedrijven die hun infrastructuur naar de cloud verplaatsen is dit een relevante ontwikkeling.

PLATFORM-CONSOLIDATIE

84% van bedrijven streeft naar unified platforms om complexiteit te reduceren [15]. EDR evolueert naar XDR als standaard: endpoint + netwerk + cloud + identity in een platform. De verschuiving van on-premise consoles naar cloud-native SaaS versnelt. Minder platforms betekent minder overhead en meer uniforme data.

> **Marktomvang:** De wereldwijde EDR-markt groeit van USD 5,1--6,4 miljard (2025) naar USD 15,5--22,0 miljard in 2030--2031, met een jaarlijkse groei van 24--27% [7]. De wereldwijde cybersecurity-uitgaven bereiken USD 240 miljard in 2026 (+12,5% versus 2025) [16].

10. Aan de slag

Je weet nu wat EDR is, wat het kost en waarom het noodzakelijk is. De volgende stap: de juiste oplossing kiezen voor jouw organisatie.

IN VIJF STAPPEN NAAR ENDPOINT SECURITY

1 Inventarisatie

Breng alle endpoints in kaart: laptops, desktops, servers, mobiele apparaten, BYOD. Elk apparaat zonder bescherming is een open deur.

2 Bepaal je model

Heb je een eigen security-team? Kies self-managed EDR. Geen team? Ga voor managed EDR (MDR). Gebruik de keuzehulp in hoofdstuk 8.

3 Selectie en pilot

Vergelijk 2--3 oplossingen op de criteria in hoofdstuk 5. Start een pilot op 10--20% van je endpoints in Detect Only modus (2--4 weken).

4 Uitrol en tuning

Rol gefaseerd uit over alle endpoints. Tune false positives, configureer exceptions en integreer met je bestaande security-stack.

5 Operationeel beheer

Definieer KPI's (MTTD, MTTR, alert noise ratio). Plan maandelijkse reviews. Documenteer alles voor NIS2-compliance.

Bronnenlijst

[1] **Diverse verzekeraarsbronnen -- 93% cyberverzekeringen eist endpoint detection (2025).** https://verzekercyber.nl/wat-zijn-de-gemiddelde-kosten-van-een-cyberaanval/

[2] **Expert Insights -- 50 Endpoint Security Stats You Should Know (2025).** 70% fileless attacks, 89% ransomware-detectie via AI. https://expertinsights.com/endpoint-security/50-endpoint-security-stats-you-should-know

[3] **CrowdStrike / Forrester -- Total Economic Impact Study 2025.** 273% ROI over 3 jaar, USD 5 miljoen benefits. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-endpoint-security-delivers-high-roi-forrester-study/

[4] **Hallo.eu -- Cybercriminaliteit kost MKB EUR 270.000 per incident.** https://hallo.eu/kennis/blogs/cybercriminaliteit-kost-mkb-euro-270-000-per-incident/

[5] **BrightDefense -- EDR vs Antivirus: What's the Difference?** Dwell time 277 dagen zonder EDR, 63% reductie met AI-driven EDR. https://www.brightdefense.com/resources/edr-vs-antivirus/

[6] **Diverse bronnen -- 60% kleine bedrijven failliet binnen 6 maanden na cyberaanval.** https://www.mkbservicedesk.nl/nieuws/ondernemersnieuws/1-op-de-5-ondernemers-had-in-2024-schade-door-cyberaanvallen

[7] **Mordor Intelligence / Grand View Research -- EDR Market Size.** USD 5,1--6,4 miljard (2025), CAGR 24--27%. https://www.mordorintelligence.com/industry-reports/endpoint-detection-and-response-market

[8] **Digitale Overheid -- Cyberbeveiligingswet (NIS2).** https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[9] **Verzeker Cyber -- Gemiddelde kosten cyberaanval Nederland.** EUR 35.000 ransomware, EUR 70.000 phishing. https://verzekercyber.nl/wat-zijn-de-gemiddelde-kosten-van-een-cyberaanval/

[10] **UnderDefense -- SentinelOne Pricing 2026.** 15--25% korting bij mid-market onderhandeling. https://underdefense.com/blog/sentinelone-pricing-2026-packages-comparison/

[11] **Vectra -- Alert Fatigue: Causes, Real Cost, and How to Fix It.** 46% false positives, 2.992 alerts/dag. https://www.vectra.ai/topics/alert-fatigue

[12] **Fortinet -- Avoid These Five Pitfalls of EDR Deployment.** https://www.fortinet.com/blog/business-and-technology/avoid-these-five-pitfalls-of-edr-deployment

[13] **Trustwave -- MDR: A Cure for Alert Fatigue.** Wanneer managed EDR noodzakelijk is. https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/managed-detection-and-response-a-cure-for-cyber-alert-fatigue-and-scalability-challenges/

[14] **NCSC -- Bereid je voor op de Cyberbeveiligingswet.** Endpoint detection als onderdeel passende maatregelen. https://www.ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[15] **Palo Alto Networks -- 2026 Predictions for Autonomous AI.** 84% streeft naar unified platforms. https://www.paloaltonetworks.com/blog/2025/11/2026-predictions-for-autonomous-ai/

[16] **Elisity -- Cybersecurity Budget 2026.** USD 240 miljard wereldwijde uitgaven. https://www.elisity.com/blog/2026-cybersecurity-budget-complete-enterprise-planning-guide