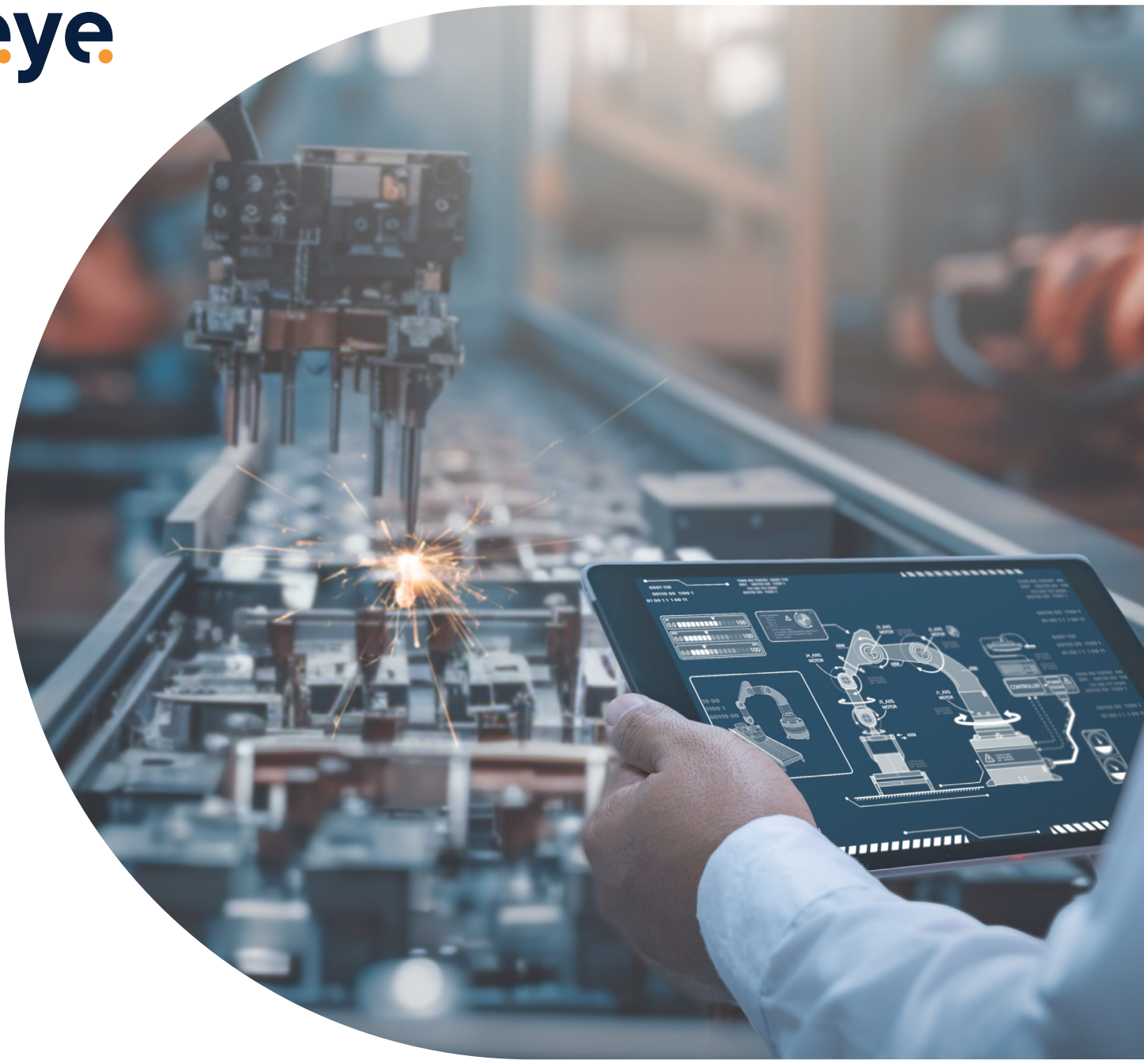

MDR Technology Evaluation Guide

EDR als solide fundament

Inhoudsopgave

Deze gids is voor IT-managers en besluitvormers die MDR-oplossingen overwegen en moeten bepalen welke technologie het fundament van hun beveiliging moet vormen: endpoints, netwerk of een combinatie van beide.

MDR-aanbieders kun je grofweg indelen in drie categorieën:

- **Endpoint Detection and Response (EDR)**
- **Network Detection and Response (NDR)**
- **Cloud Detection and Response (CDR)**

Veel aanbieders bieden een vorm van Extended Detection and Response (XDR) aan en noemen hun dienst Managed XDR (MXDR). Deze diensten combineren signalen van verschillende beveiligingsoplossingen en correleren deze met data van EDR of NDR. Toch vormt één van deze twee technologieën de basis van de service. Het is aan jou om te bepalen welke het beste past bij jouw organisatie.

EDR vs. NDR: Wat zijn de verschillen?

EDR	NDR
EDR richt zich op individuele apparaten zoals laptops, desktops en servers. Het monitort activiteiten op het niveau van het apparaat, waaronder bestanden, processen, gebruikers en netwerkverkeer. Dit is vaak het punt waar bedreigingen beginnen en zich verder verspreiden.	NDR legt de focus op het netwerkverkeer. Het analyseert datastromen binnen en buiten het netwerk om afwijkingen of bedreigingen te detecteren. Denk hierbij aan interne verbindingen (east-west) en externe communicatie (north-south).

Waarom is je keuze voor een basisbeveiligingstechnologie zo belangrijk?

Misschien denk je: “Ik besteed de detectie en respons toch uit, waarom zou de technologie belangrijk zijn?” Maar er zijn twee goede redenen om hier aandacht aan te besteden:

Verklein de kans op een succesvolle aanval

De snelheid waarmee je MDR-provider reageert, bepaalt vaak of een aanval succesvol is of tijdig wordt ingeperkt. De volgende vragen zijn daarbij essentieel:

- Hoe effectief is de detectie? Worden bedreigingen in elke fase van een aanval herkend?
- Hoe snel worden signalen geanalyseerd en aan elkaar gekoppeld?
- Hoe accuraat zijn de meldingen? Voorkom je onnodige valse waarschuwingen?
- Is er voldoende context om een dreiging snel te onderzoeken?
- Hoe snel en flexibel kun je reageren om de impact op je bedrijfsvoering te minimaliseren?
- Welke tools krijg je voor onderzoek en herstel na een incident?

Je team moet vertrouwd zijn met de fundamentele producten

Je besteedt niet je volledige cybersecurityprogramma uit – alleen onderdelen van detectie en respons. Je blijft zelf betrokken bij bepaalde activiteiten, afhankelijk van

de gekozen provider en de technologie die zij als basis gebruiken. Het is daarom cruciaal dat je kiest voor een provider die werkt met producten waarmee jij en je team vertrouwd zijn, gebaseerd op jullie ervaring en expertise. Deze gids helpt je antwoord te vinden op de volgende vragen:

- Hoe ingewikkeld is de implementatie van de detectie- en responsproducten?
- Moet ik extra agents, sensoren of probes installeren?
- Moet ik integraties configureren met andere beveiligingstools en applicaties?
- Hoeveel inspanning is er van mijn kant nodig tijdens een aanval om informatie aan te leveren die de provider niet zelf kan bereiken?
- Hoeveel werk vereist onderzoek en herstel na een aanval, en welke tools en informatie worden hiervoor beschikbaar gesteld?

Implementatiestappen en zichtbaarheid

Zichtbaarheid is alles in beveiliging. Zonder duidelijk zicht op potentiële dreigingen is het bijzonder moeilijk om proactief actie te ondernemen. **EDR biedt diep inzicht** in host-gedrag in Windows-, Linux- en macOS-systemen. Dit omvat ook (virtuele) servers en laptops, onafhankelijk van waar ze staan. **NDR biedt uitgebreid inzicht in netwerkgedrag via een centraal apparaat, wat bepaalde voor- en nadelen met zich meebrengt.**

	EDR	NDR
Implementatiemethode	Agentsoftware-implementatieprofiel geconfigureerd in gangbare MDM-oplossingen zoals Intune of AD Group Policy.	Virtueel of hardware-apparaat, centrale locatie in het netwerk, passieve SPAN-poort of in-line (komt minder voor).
Gefaseerde implementatie	Agents worden meestal geïmplementeerd in een leer- of passieve modus, wat een baseline voor gedrag creëert, terwijl processen niet gepauzeerd of onderbroken worden (en er dus minder impact is op de business).	Het NDR-implementatieplan moet opgesteld worden op basis van de lokale netwerkarchitectuur. Meerdere IT-stakeholders moeten firewalls aanpassen en hardware-onderhoudsprocessen toevoegen aan het team.
Time-to-Value (TTV)	Zodra het agent-installatieprofiel is uitgerold, worden alle beheerde endpoints binnen enkele minuten tot uren aangemeld.	Een NDR-implementatie duurt doorgaans enkele weken of maanden.

Zicht-baarheid (telemetrie)	EDR monitort en verzamelt processen, draaiende applicaties, bestandswijzigingen, gebruikersactiviteit, cloud-verbindingen, naburige apparaten en zelfs **netwerkverbindingen van en naar het apparaat.** De meest geavanceerde EDR-oplossingen combineren de telemetrie van alle agents in één centraal IT-overzicht.	Afhankelijk van de netwerkarchitectuur monitort en verzameld de NDR netwerk-metadata, zoals bron-IP-adressen, bestemmings-IP-adressen en bijbehorende poortnummers. Bij sNAT is het bron-IP-adres niet beschikbaar. **Relevante datavelden zijn vaak versleuteld met TLS** wanneer SSL-offloading niet geïmplementeerd is.
Aandacht-spunten bij correcte im-plementaties	EDR-dekking is essentieel voor voldoende inzicht om onbeheerde endpoints (Shadow IT) te minimaliseren. **Asset discovery-telemetrie,** beschikbaar in de meeste toonaangevende EDR-oplossingen, moet worden gebruikt om de EDR-dekking naar bijna 100% te brengen. Vergeet niet om de **EDR-verwijderings-beveiliging** in te schakelen.	Forceer **always-on VPN** in hybride omgevingen, anders worden remote werknemers niet gezien. Overweeg het **ontsleutelen van verkeer met SSL-of-floading,** anders blijven detecties waarschijnlijk onbruikbaar zonder context. **Voorkom creatie van (onveilige) routes** tussen gesegmenteerde netwerken naar NDR, aangezien dit mogelijk de waarde van de segmentatie elimineert.

Detecteren van moderne cyberdreigingen

De jaarlijks bijgewerkte ENISA Threat Landscape (ETL) benadrukt dat ransomware-, phishing- en toeleveringsketenaanvallen tot de meest significante huidige uitdagingen voor organisaties horen. Het detecteren van deze dreigingen vereist een delicate balans tussen het maximaliseren van detectiemogelijkheden en het minimaliseren van fout-positieven, om alertmoeheid te voorkomen. EDR en NDR bieden ieder andere waarde bij het detecteren van deze moderne bedreigingen.

	EDR	NDR
Laterale beweging	Volgt ongebruikelijke interne verbindingen, escalaties van privileges en procesafwijkingen op endpoints. Kan het detecteren als aanvallers tussen apparaten proberen te bewegen of privileges proberen te escaleren.	Afhankelijk van de netwerkarchitectuur monitort NDR verkeer tussen interne hosts op ongebruikelijke verbindingen of datastromen. Triage op deze waarnemingen is lastig, vanwege het gebrek aan endpoint-context.
Ransomware	Detecteert grootschalige bestandsversleuteling via bestandssys-teemmonitoring en gedragsanalyse. Isoleert gecompromitteerde endpoints en stopt malafide processen.	Monitort ongebruikelijk uitgaand verkeer naar C2-servers, maar heeft moeite om fout-positieven te beperken, vanwege TLS en omdat de levensduur van de C2-infrastructuur erg kort is (enkele minuten tot dagen).

Phishing (pogingen)	Monitort e-mailclients en browsers om malafide bijlagen of URL's te onderscheppen. Detecteert pogingen om inloggegevens te stelen en blokkeert installatie van malafide software.	Identificeert ongebruikelijk netwerkverkeer of DNS-verzoeken naar phishing-domeinen. Beperkt in het voorkomen van initiële inbreuken en HTTPS-afdwinging door browsers.
Toelev-eringskete-naanvallen	Monitort gecompromitteerde applicaties op ongebruikelijk gedrag en gebruikt IOC's om te detecteren of vertrouwde software zich malafide gedraagt.	Detecteert onverwachte communicatie van gecompromitteerde software. Heeft moeite met onderscheid maken tussen legitiem verkeer en malafide verkeer als er geen endpoint-context is.
Exploitatie (pogingen)	Detecteert exploitatiepogingen aan de hand van gedragsanalyse en dreigingsinformatie. Biedt realtime waarschuwingen en kan de endpoint isoleren.	Houdt netwerkanomalieën in de gaten die duiden op misbruik, maar heeft moeite met aanvallen die uitsluitend op hostniveau plaatsvinden.
Data (kroonjuweel)	Endpoints bevatten of beheren vaak de kroonjuwelen (zoals data) die aanvallers zoeken. Zelfs als eerdere detectiepogingen gemist worden, zorgt EDR ervoor dat er meerdere kansen langs het aanvalspad zijn om de aanvaller te identificeren en te stoppen, voordat er significante schade gedaan wordt.	Monitort op verdachte data-overdrachten en netwerkcommunicatie die mogelijk gericht zijn op gevoelige assets. Maar NDR mist inzicht in specifieke acties die op de endpoints plaatsvinden, die gemakkelijk gezien kunnen worden als goedaardige IT-beheeractiviteiten zoals het maken van backups. Zodra de dataexfiltratie naar externe IP-adressen gedetecteerd wordt, is het vaak al te laat.

Reactiemogelijkheden om actieve dreigingen te mitigeren

Detectie is slechts één onderdeel van EDR en NDR. De mogelijkheid om effectief te reageren is wat een oplossing echt krachtig maakt.

- **EDR biedt geavanceerde reactiemogelijkheden** die veel verder gaan dan alleen beveiligingsteams op de hoogte stellen. Het biedt directe interventies, waaronder het isoleren van een endpoint, beëindigen van malafide processen en wijzigingen die door malware gedaan zijn terugrollen. Dit stelt organisaties in staat om dreigingen te beperken en neutraliseren voor ze escaleren tot een inbraak.
- **De reactiemogelijkheden van NDR zijn daarentegen beperkt.** NDR kan doorgaans alleen TCP-resetpakketten sturen om verdachte verbindingen te verstoren, wat de onderliggende dreiging niet wegneemt. Het resultaat is vaak een vertraging in het herstel, aangezien de daadwerkelijke oorzaak van de dreiging actief blijft. Bovendien kan het uitdagend zijn om zonder het gedetailleerde inzicht dat EDR biedt, vast te stellen welk apparaat de bron is van malafide netwerkactiviteit, zeker in complexe of slecht gedocumenteerde netwerkomgevingen.

In praktische beveiligingsworkflows **wisselen analisten vaak van NDR naar EDR** als ze de diepgang en context van een waarschuwing moeten begrijpen. NDR signaleert misschien verdacht verkeer, maar zonder inzicht op endpoint-niveau is het lastig om het volledige verhaal te bepalen – bijvoorbeeld welk proces het gedrag initieerde of dat er malafide veranderingen hebben plaatsgevonden. EDR vult dit gat in door de diepgang te bieden die nodig is voor effectieve, geïnformeerde reacties.

Veelvoorkomende misvattingen

Een veelvoorkomende misvatting is dat **NDR, omdat het out-of-band is,** fraudebestendig is en daarom een veiligere optie is voor netwerkbeveiliging. Aanvallers vinden het mogelijk moeilijker om NDR uit te schakelen, omdat het los van de endpoints opereert. Maar dat maakt het niet onverslaanbaar. Aanvallers kunnen NDR omzeilen door versleutelde communicatie of vertrouwde platformen als GitHub te gebruiken om malware te verspreiden – waardoor NDR niet meer in staat is om hun activiteit te monitoren.

EDR's bescherming tegen manipulatie op kernelniveau verzekert daarentegen dat het functioneel blijft, zelfs als een aanvaller beheerdersrechten op een gecompromitteerd apparaat krijgt. Probeert iemand de agent te manipuleren, dat wordt er een kritieke waarschuwing getriggerd. Het is wel zo dat er software bestaat die EDR kan stoppen. Maar als een aanvaller dit wil inzetten, zijn vaak beheerdersrechten op een endpoint nodig, wat betekent dat EDR meerdere detectiekansen heeft langs het aanvalspad naar de admin.

Een ander argument voor NDR is de waarde die het biedt bij het monitoren van omgevingen waar endpoint agents niet geïmplementeerd kunnen worden, bijvoorbeeld bij OT-, IoT- en legacy-systemen. Maar deze systemen representeren doorgaans slechts een klein deel van de gehele infrastructuur en zijn beperkt blootgesteld aan het netwerk. De meer effectieve strategie is om deze legacy-systemen te isoleren en de IT-infrastructuur daar omheen te beschermen met EDR, zodat je zeker bent dat aanvallers zich niet naar de meer kritieke systemen kunnen bewegen.

Daar komt bij dat hoewel **NDR inzicht biedt in netwerk-gebaseerde aanvallen,** de meeste aanvallen tegenwoordig endpoint-gebaseerd zijn. Deze aanvallen gebruiken meestal remote access-methoden om via het internet in te breken op systemen. In onze incident response-ervaring hebben aanvallen zoals ransomware altijd te maken met inbreuk op afstand, waarbij endpoints het toegangspunt zijn. **EDR is perfect uitgerust voor deze scenario's,** doordat het uitgebreide detectie- en reactiemogelijkheden biedt.

Conclusie: EDR als kern, NDR als aanvulling

Na het evalueren van de mogelijkheden en beperkingen van zowel EDR als NDR, wordt duidelijk waarom **EDR de hoeksteen** is van effectieve cybersecuritystrategieën. EDR biedt realtime inzicht, geavanceerde reactiemogelijkheden en de context die nodig is om dreigingen te detecteren en mitigeren – wat allemaal essentieel is in het huidige snel veranderende dreigingslandschap.

Hoewel **NDR een ondersteunende rol kan spelen** – het biedt aanvullende detectie op afwijkingen bij onbeheerde apparaten of laterale bewegingen binnen specifieke netwerkarchitecturen – moet het niet gezien worden als de voornaamste oplossing. **NDR is het meest effectief als het EDR aanvult,** waarbij het blinde vlekken in complexe omgevingen helpt wegnemen. Maar het komt tekort in de detectie, reactie en algehele operationele effectiviteit in vergelijking met de endpoint-focus die EDR heeft.

Om de beste resultaten te bereiken, moeten organisaties zich richten op de implementatie van een **geavanceerde managed EDR-oplossing** en zich verzekeren dat het goed geconfigureerd is met effectieve manipulatiebescherming en incident response-draaiboeken. **NDR moet gezien worden als optionele laag,** die alleen ingezet wordt als er specifieke inzichtvereisten zijn die alleen EDR niet kan vervullen.

Case Studies

KeyTec Netherlands

Toen het aantal ransomware-aanvallen in hun sector sterk steeg, besloot maakbedrijf KeyTec actie te ondernemen. Ontdek hoe Eye Security hen hielp hun verdediging proactief te versterken en een cyberbewuste werkcultuur te creëren.

Signature Foods

Nu cybercriminaliteit steeds geavanceerder wordt, wenden bedrijven zich tot externe partners om bij te blijven. Ontdek hoe Eye Security Signature Foods binnen enkele weken complete cyberbeveiliging bood.

Bij Eye Security adviseren we een no-nonsenseaanpak voor cybersecurity. Een aanpak die de nadruk legt op de basisprincipes, prioriteit geeft aan endpoint-verdediging en netwerkmonitoring selectief gebruikt om de hiaten op te vullen. Door dit te doen, helpen we een veerkrachtige beveiligingsaanpak op te bouwen die aanvallers voorblijft en zich aanpast aan opkomende bedreigingen.

Visit www.eye.security