previder

De kracht van
Previder Managed XDR

Maximale cybersecurity, minimale zorgen

it starts here.

Inhoudsopgave

1. 24/7 beveiliging zonder zorgen

In een tijdperk waarin digitale transformatie de drijvende kracht is achter zakelijke groei, staan organisaties meer dan ooit bloot aan cyberdreigingen. Van ransomware-aanvallen tot datalekken en phishing-campagnes. Deze bedreigingen worden niet alleen complexer, maar ook frequenter. De harde realiteit? Geen enkele organisatie is immuun.

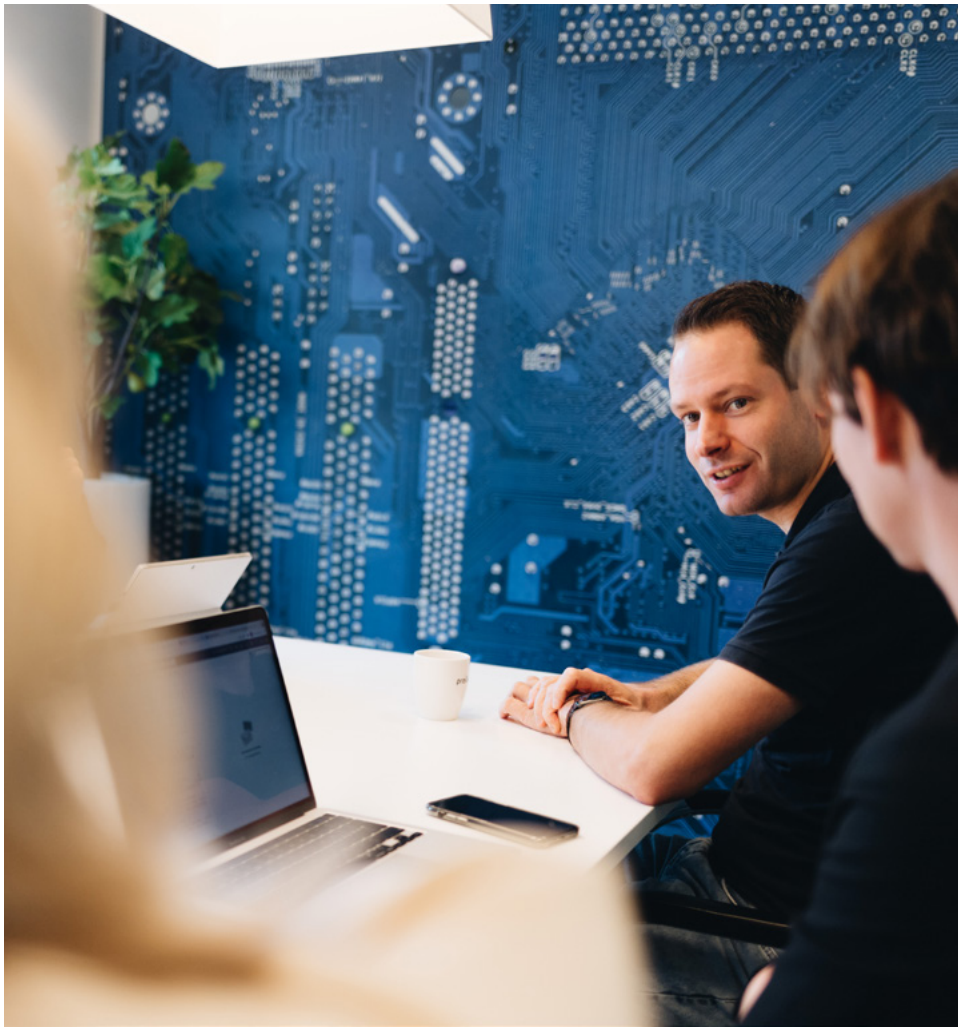
De traditionele benaderingen schieten vaak tekort. Ze missen de snelheid en intelligentie om complexe dreigingen real-time te identificeren en te neutraliseren. Bovendien worden veel IT-teams overspoeld door meldingen, waardoor kritieke aanvallen gemakkelijk over het hoofd kunnen worden gezien.

Als CIO, CTO, CFO, CISO of IT-manager ben je verantwoordelijk voor het beschermen van je organisatie tegen deze risico's. Maar hoe doe je dat effectief, zonder je team te overbelasten, te verdrinken in dure tools of constant achter de feiten aan te lopen?

Dit is waar **Managed Extended Detection and Response (MXDR)** het verschil maakt. Met MXDR krijg je geavanceerde cybersecurity zonder de kosten en complexiteit van een eigen Security Operations Center (SOC). Previder Managed XDR beschermt jouw organisatie 24/7 tegen cyberdreigingen, zodat jij je kunt focussen op groei en innovatie.

In deze whitepaper laten we je zien hoe Previder Managed XDR je kan helpen om voorop te blijven in de strijd tegen cyberdreigingen. We bespreken wat MXDR is, welke voordelen het biedt en wat de risico's zijn als je niets doet. Dit is jouw kans om de cybersecurity-uitdagingen van vandaag aan te pakken en je organisatie toekomstbestendig te maken.

Ben je klaar om de controle terug te nemen? Lees verder en ontdek hoe Previder Managed XDR je helpt om risico's te minimaliseren en je gemoedsrust te maximaliseren.



2. Van reactief naar proactief: de kracht van Managed XDR

2.1 Dagelijkse uitdagingen in cybersecurity

De wereld van cyberdreigingen verandert snel. Hackers maken gebruik van steeds geavanceerdere technieken, terwijl traditionele beveiligingstools vaak tekortschieten. Veel organisaties vertrouwen nog op firewalls, antivirussoftware en SIEM-oplossingen, maar deze tools opereren meestal los van elkaar. Ze bieden reactieve beveiliging en missen de kracht om complexe dreigingen te detecteren voordat het te laat is. Door deze toenemende complexiteit lopen veel organisaties tegen dezelfde problemen aan:

- **Tekort aan capaciteit en expertise:** interne IT- en beveiligingsteams hebben vaak beperkte capaciteit en een tekort aan specialistische kennis om 24/7 monitoring en incidentrespons uit te voeren.
- **Toename van geavanceerde dreigingen:** dreigingen zoals ransomware, phishing en supply chain aanvallen worden steeds geavanceerder en omzeilen traditionele beveiligingsmaatregelen.
- **Complexiteit van hybride IT-omgevingen:** de combinatie van on-premise, cloud en SaaS-applicaties maakt beveiliging complex en vergroot risico's.
- **Strengere compliance-eisen en risico's:** strengere regelgeving (zoals GDPR, ISO 27001, NIS2) vraagt om real-time monitoring en incidentrapportage.
- **Hoge kosten & inefficiëntie:** de inzet van meerdere beveiligingstools zonder integratie leidt tot hoge kosten en een inefficiënte beveiligingsstrategie.

2.2 Wat is Managed XDR?

Managed Extended Detection and Response (MXDR) is een alles-in-één beveiligingsoplossing die AI gedreven detectie combineert met menselijke expertise. MXDR analyseert continu data uit je hele IT-omgeving en detecteert afwijkingen of potentiële bedreigingen. Vervolgens worden deze bedreigingen snel geïdentificeerd, geprioriteerd en opgelost.

"MXDR analyseert continu data uit je hele IT-omgeving en detecteert afwijkingen of potentiële bedreigingen."

- **Geavanceerde detectie:** door middel van AI, machine learning en threat intelligence detecteert MXDR zowel bekende als onbekende dreigingen real-time.
- **Geautomatiseerde en manuele incidentrespons:** MXDR reageert snel en effectief op cyberdreigingen om schade te minimaliseren.
- **Continue monitoring en threat hunting:** MXDR biedt 24/7 monitoring en proactieve threat hunting om verdacht gedrag vroegtijdig te signaleren en te elimineren.
- **Compliance en rapportage:** MXDR helpt organisaties te voldoen aan regelgeving zoals ISO 27001 en GDPR door uitgebreide forensische analyses en rapportages te leveren.

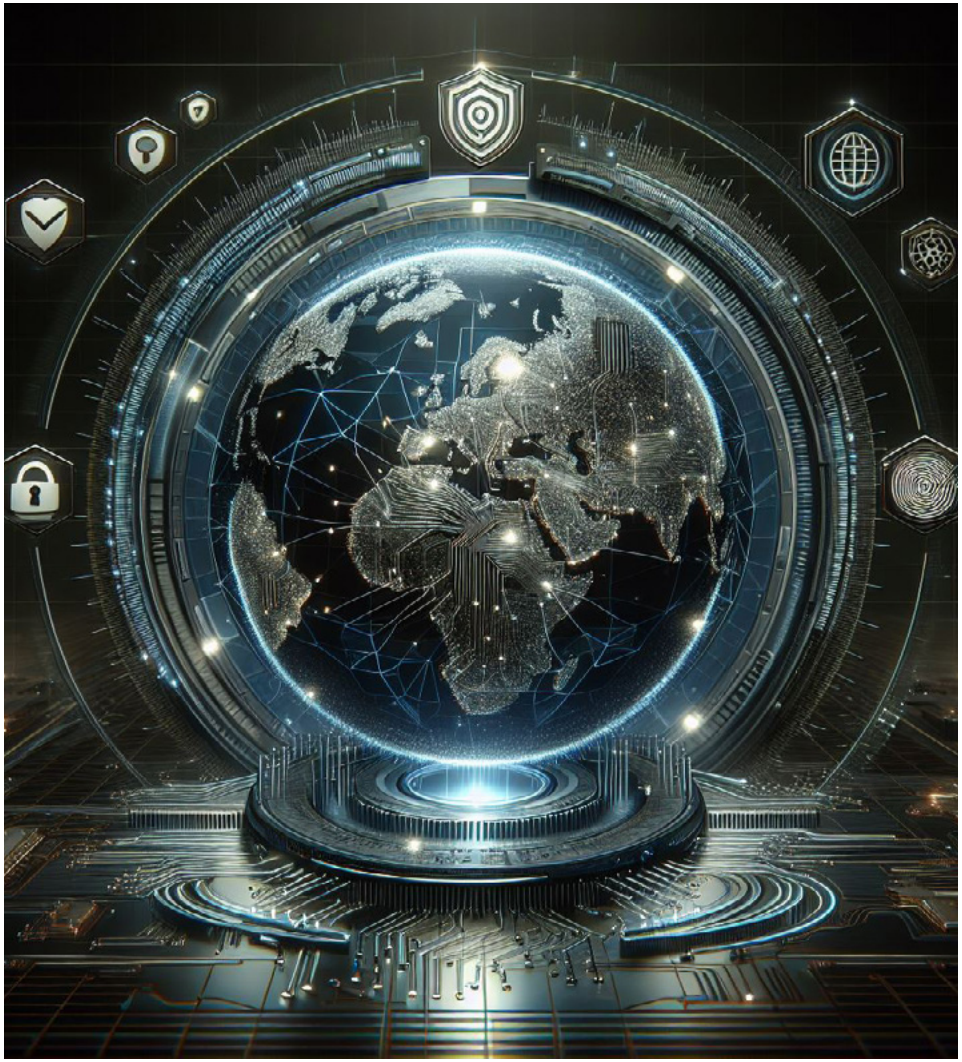
2.3 Welke risico's loop je zonder MXDR?

Waarom kiezen voor MXDR? Omdat geen enkele organisatie immuun is voor cyberdreigingen en traditionele beveiliging simpelweg niet meer volstaat. Cyberdreigingen ontwikkelen zich razendsnel, en zonder de juiste bescherming loopt jouw bedrijf dan ook aanzienlijke risico's:

- **Onopgemerkte bedreigingen:** zonder 24/7 monitoring blijven bedreigingen vaak te lang onopgemerkt, wat de impact van een aanval vergroot.
- **Financiële schade:** een datalek of cyberaanval kan leiden tot hoge kosten voor herstelwerkzaamheden, dataverlies, schadeclaims van klanten of zelfs operationele verliezen (downtime).
- **Reputatieschade:** een datalek of beveiligingsincident kan het vertrouwen van klanten, partners en investeerders ernstig schaden. Voor veel bedrijven betekent een beschadigde reputatie een verlies van marktaandeel en inkomsten.
- **Compliance-risico's:** niet voldoen aan regelgeving zoals AVG en NIS2 kan leiden tot sancties en juridische gevolgen.
- **Complexiteit:** zonder voortdurende beveiliging en incidentrespons is snel en adequaat reageren op een bedreiging onmogelijk, wat je een doelwit maakt voor aanvallers.

Zonder MXDR neem je onnodige risico's: hoe lang zou jouw organisatie kunnen overleven zonder toegang tot belangrijke systemen of data?

→ Previder Managed XDR



3. Previder Managed XDR: complete cybersecurity, volledig ontzorgd

Previder Managed XDR – aangeboden in samenwerking met onze oficiële partner Eye Security – is een geavanceerde, volledig beheerde cybersecurity-oplossing die bedrijven helpt om bedreigingen te detecteren, te onderzoeken en hierop te reageren. Waar traditionele beveiliging vaak reactief is, biedt MXDR proactieve bescherming door gebruik te maken van geavanceerde technologieën zoals Artificial Intelligence (AI), machine learning en uitgebreide dataverzameling. MXDR combineert endpoint-, netwerk-, cloud- en gebruikersgegevens om een compleet overzicht van je digitale omgeving te geven en bedreigingen in een vroeg stadium te stoppen. Je krijgt niet alleen inzicht in potentiële kwetsbaarheden, maar ook een direct actieplan voor incidentrespons, waardoor je bedrijfscontinuïteit gewaarborgd blijft.

Met Previder Managed XDR tackle jij alle security-uitdagingen in één keer en bied jij je organisatie de bescherming die het nodig heeft, zonder extra last op eigen schouders. Ons high-end Security Operations Center (SOC) bewaakt je systemen 24/7, grijpt direct in bij verdachte activiteiten en zorgt ervoor dat je voldoet aan wet- en regelgeving zonder extra druk op je IT-afdeling.

- **24/7 Security Operation Center (SOC):** proactieve monitoring door een team van experts dat continu toezicht houdt, adequaat reageert en dreigingen en incidenten minimaliseert.
- **Attack Surface Management (ASM):** continue monitoring van jouw aanvalsoppervlak en directe actie bij de detectie van een kritieke kwetsbaarheid.
- **Eye Anti-Spoofing Tool (EAST):** visuele bescherming tegen spoofing van Microsoft-inlogpagina's om malafide pagina's te herkennen en gebruikers te beschermen.
- **Threat Hunting:** snelle identificatie van kritieke kwetsbaarheden door threat intelligence analisten en een direct reactie op dreigingen.
- **Incident Response (IR):** directe hulp bij incidenten, inclusief on-site ondersteuning door een incident response team dat 24/7 beschikbaar is.
- **Management Reporting:** volledig eigenaarschap van incidenten en transparante rapportage inclusief aanbevelingen voor het verbeteren van je cyberweerbaarheid.

3.1 Previder Managed XDR voor jouw organisatie

Bij Previder geloven we dat technologie alleen effectief is wanneer het naadloos wordt geïntegreerd in jouw bedrijfsprocessen. Doordat we onze diensten volledig afstemmen op de behoeften van jouw organisatie en sector, profiteer je van oplossingen die niet alleen generiek en effectief, maar specifiek voor jouw situatie ontworpen zijn.

Waar Eye Security technologie levert, nemen wij het volledige operationele eigenaarschap over jouw beveiliging. Wij zijn jouw **single point of contact** voor alles wat met cyberbeveiliging te maken heeft, van implementatie en monitoring tot incidentrespons en managementrapportage. Minder schakels betekent snellere communicatie en actie.

Zorg er met Previder Managed XDR voor dat jij je kunt focussen op de groei van je bedrijf zonder zorgen over de veiligheid van je data:

- **Altijd beschermd:** 24/7 monitoring en snelle incidentrespons houden je organisatie veilig, ook buiten kantooruren.
- **Proactieve beveiliging:** minimale impact van incidenten door tijdige en directe actie.
- **Kostenbesparend & efficiënt:** voorkom dure herstelkosten en downtime door detectie in een vroeg stadium, zonder te investeren in een eigen SOC.
- **Schaalbaar & toekomstbestendig:** een flexibele oplossing die met je bedrijf meegroeit, ongeacht de omvang van je bedrijf.
- **Inzicht & compliance:** door de integratie van verschillende beveiligings-lagen krijg je een holistisch beeld van je IT-omgeving en voldoe je moeiteloos aan regelgeving als NIS2 en GDPR.

3.2 Hoe werkt Previder Managed XDR?

Met Previder Managed XDR ben je dus altijd een stap voor op aanvallers en heb jij geen zorgen meer over ontbrekende expertise of overbelaste IT-teams: wij nemen de volledige cybersecurity zorg uit handen, zodat jij je kunt focussen op groei en innovatie.

- **Intake en beoordeling:** samen bepalen wij jouw beveiligingsbehoeften en stellen een plan op.
- **Implementatie:** binnen 24 uur actief, zonder verstoring van jouw systemen.
- **Continu beveiligd:** wij blijven 24/7 monitoren, reageren en adviseren.

Door te kiezen voor onze Managed XDR-dienst krijg je niet alleen toegang tot geavanceerde cybersecurity-technologie, maar ook tot een partner die jouw veiligheid als topprioriteit beschouwt. Onze expertise en operationele kracht zorgen ervoor dat jij niet alleen beschermd bent tegen bedreigingen, maar ook in staat bent om te groeien zonder zorgen over je digitale veiligheid.

“Overtuigd van onze Managed XDR oplossing? Start eenvoudig binnen 24 uur!”

Inzicht krijgen in je kwetsbaarheden? Neem contact met ons op en ontdek hoe Previder Managed XDR jouw organisatie naar een hoger securityniveau tilt!

→ Contact

Over Previder

Samen met ruim 300 IT-specialisten en vanuit onze eigen datacenters leveren wij het gehele IT-fundament voor organisaties. Van digitale werkplekken tot aan het managen van complexe cloudomgevingen. Wij weten de juiste specialist op de juiste plek te zetten en staan met onze persoonlijke aanpak, betrokkenheid en directe lijnen 24/7 klaar om jouw organisatie te helpen met IT-vragen.

Benieuwd wat Previder voor jouw organisatie kan betekenen?
We praten er graag eens met je over. Neem contact op voor een vrijblijvende kennismaking.

088 - 332 3333 **info@previder.nl**

previder

088 - 332 3333 www.previder.nl

it starts here.