SOPHOS

EBOOK

EDR, XDR, MDR

Quelle est la différence ?
Quelle solution convient à votre entreprise ?

SOMMAIRE

Introduction 3

Qu’est-ce que l’EDR? 4

Qu’est-ce que le XDR? 5

Qu’est-ce que le MDR? 6

Quand envisager une solution EDR, XDR ou MDR 7

Autres éléments à considérer avant toute décision 8

En conclusion 9

EDR, XDR, MDR

Quelle est la différence? Quelle solution convient à votre entreprise?

Les responsables informatiques et cybersécurité font face à une pression croissante pour renforcer la cyber-résilience de leur organisation sans surcharger des équipes ou des budgets déjà limités. Face à l'augmentation du nombre de menaces et à la sophistication croissante des attaques, il est impératif d'investir intelligemment dans des capacités de détection et de réponse.

Que vous opériez à l'échelle mondiale ou que vous gériez une équipe restreinte, il est essentiel d'aligner votre approche en matière de cybersécurité sur le profil de risque et les réalités opérationnelles de votre organisation. Pour de nombreux dirigeants, choisir la bonne approche de détection et de réponse aux incidents signifie également décider s'il faut la gérer soi-même ou solliciter un partenaire de confiance. Les solutions EDR (Endpoint Detection and Response), XDR (Extended Detection and Response) et MDR (Managed Detection and Response) offrent chacune des avantages uniques, mais le véritable défi est d'identifier celle qui apporte le plus de valeur à votre organisation. Les solutions EDR et XDR sont des outils qui aident votre équipe à détecter, à investiguer et à répondre plus rapidement aux menaces. Une solution MDR est un service fournit par des experts en analyse qui surveillent et répondent aux menaces 24 h/24 et 7 j/7, en utilisant des outils XDR et d'autres technologies.

Comprendre ce qui distingue ces approches et comment elles peuvent se compléter est la première étape vers l'élaboration d'une stratégie de cybersécurité qui vous protège aujourd'hui et prépare votre résilience pour demain.

L'importance de la détection et de la réponse

Une protection Endpoint robuste reste une première ligne de défense indispensable. Or les acteurs malveillants sophistiqués exploitent des identifiants légitimes, usurpent l'identité d'utilisateurs de confiance et abusent des outils informatiques natifs pour contourner les défenses. Pour un outil de prévention unique et isolé, ces attaques n'apparaissent pas nécessairement comme malveillantes et c'est précisément pour cette raison qu'elles parviennent à leurs fins.

Les capacités de détection et de réponse, telles que fournies par les solutions EDR, XDR et MDR, comblent cette lacune critique. Elles aident à identifier et à neutraliser les menaces qui échappent à la prévention avant qu'elles ne puissent se transformer en incidents majeurs.

QU'EST-CE QUE L'EDR ?

Une solution EDR (Endpoint Detection and Response) s'inscrit dans une stratégie de sécurité Endpoint globale. Elle aide les équipes à surveiller, à détecter et à répondre aux menaces et aux incidents de sécurité sur les appareils, tels que les ordinateurs portables, les ordinateurs de bureau et les serveurs.

Avantages clés d'une solution EDR :

Elle offre une visibilité en temps réel sur l'activité des postes, telle que l'exécution de fichiers, le comportement des processus et les mouvements latéraux, pour permettre aux équipes de rapidement détecter et neutraliser les menaces avant qu'elles ne se propagent.

Elle détecte les menaces évasives en identifiant les indicateurs comportementaux, vous aidant ainsi à détecter les attaques que les outils de prévention traditionnels manquent souvent.

Elle automatise les actions de réponse telles que l'isolement des appareils affectés ou l'arrêt des processus malveillants, réduisant ainsi le temps d'exposition et empêchant les attaquants d'obtenir un accès supplémentaire.

Découvrez comment Sophos EDR protège vos postes et vos serveurs contre des attaques sophistiquées, qu'ils se situent au bureau, sur le réseau ou dans le cloud.

QU'EST-CE QUE LE XDR ?

Une solution XDR (Extended Detection and Response) améliore la visibilité sur les menaces en intégrant les données provenant de l'ensemble de votre écosystème de sécurité, au-delà des postes et des serveurs. Elle prend en compte les données des pare-feux, de la messagerie, de l'infrastructure cloud, des systèmes de gestion de l'identité, des solutions de sauvegarde et de restauration, des outils de productivité, en plus des postes et des serveurs, et bien plus encore. Une solution XDR permet de corréler plus efficacement les activités suspectes, contribuant ainsi à identifier les attaques multi-vecteurs sophistiquées que des outils cloisonnés pourraient ne pas détecter.

Alors que l'EDR examine en profondeur les postes, les fonctionnalités XDR étendent la visibilité et font le lien entre tous les systèmes. Elles offrent une vue d'ensemble d'une attaque, facilitant ainsi la détection des menaces multi-étapes et multi-vecteurs qui, autrement, passeraient inaperçues.

Avantages clés d'une solution XDR :

Elle corrèle les signaux provenant de plusieurs vecteurs d'attaque afin d'identifier les modèles et de prioriser les alertes de haute fidélité. Cela réduit le bruit de fond et met en lumière des menaces complexes et multi-systèmes.

Elle optimise les processus d'investigation pour une réponse plus rapide et plus efficace de votre équipe. Les analystes obtiennent une visibilité claire sur le déroulement d'une attaque et sur les mesures à prendre pour éviter qu'elle ne se reproduise.

Elle assiste les processus d'investigation et de réponse grâce à des outils basés sur l'IA qui accélèrent l'analyse et la remédiation des incidents, permettant ainsi une résolution plus rapide et plus fiable.

Découvrez comment Sophos XDR vous permet de détecter, d'investiguer et de répondre aux activités suspectes à travers l'ensemble de votre écosystème.

QU'EST-CE QU'UN SERVICE MDR ?

Un service MDR (Managed Detection and Response) est un SOC managé qui combine IA et expertise humaine afin d'assurer la surveillance, la chasse aux menaces et la réponse aux incidents, 24 heures sur 24 et 7 jours sur 7. Un tel service est particulièrement utile pour les organisations qui ne fonctionnent pas 24 h/24 et 7 j/7, ou celles qui sont confrontées à des lacunes dans la couverture de leur SOC, à des difficultés de recrutement de personnel qualifié ou à une complexité croissante.

Un service MDR peut fonctionner comme une solution entièrement externalisée ou une extension co-managée de votre SOC interne, contribuant ainsi à réduire le temps de séjour des menaces et à bloquer les incidents, tels que les ransomwares, avant qu'ils ne s'aggravent.

Avantages clés d'un service MDR :

Une couverture 24/7. Les menaces ne respectent pas les horaires de bureau classiques : 88 % des attaques de ransomware se produisent en dehors des heures de bureau normales. Un service MDR garantit une couverture à toute heure du jour et de la nuit.

Vous bénéficiez de l'expertise d'analystes en cybersécurité qui comprennent le comportement des attaquants et agissent de manière décisive. Ces spécialistes gèrent des incidents quotidiennement, en priorisant et en contenant les menaces afin d'assurer le bon fonctionnement de votre entreprise.

Pas de surproduction d'alertes ni de tri manuel. Un service MDR élimine le bruit de fond, pour que votre équipe puisse se concentrer sur vos initiatives stratégiques plutôt que de perdre leur temps à examiner de faux positifs.

Une résolution rapide dans les moments les plus critiques. Dans le cas d'incidents à haut risque tels que les ransomwares, les équipes MDR peuvent détecter et contenir les menaces avant même que les équipes internes n'en aient eu connaissance, ce qui permet d'éviter des perturbations opérationnelles et de réduire les risques.

Découvrez comment Sophos MDR, avec sa plateforme ouverte optimisée par l'IA et son équipe d'experts en analyse, peut compléter votre équipe et vous rejoindre là où vous en êtes dans votre parcours de cybersécurité.

QUAND ENVISAGER UNE SOLUTION EDR, XDR OU MDR

Solution	Envisagez cette option si...	Peut ne pas convenir si...
EDR	• Vous avez besoin d'une détection et d'une réponse robustes au niveau de vos terminaux. • Vous souhaitez renforcer vos défenses au-delà des outils de protection Endpoint préventifs. • Vous mettez en place une défense multicouche capable de prendre en charge l'intégration future de solutions XDR ou MDR.	• Vous avez besoin d'une visibilité plus étendue sur l'ensemble de votre environnement (cloud, identité, réseau, sauvegarde, etc.). • Vous aspirez à une détection et une réponse 24/7, sans externalisation ni augmentation de vos effectifs.
XDR	• Vous avez besoin d'une vue unifiée sur tous les vecteurs d'attaque clés, y compris les terminaux, les pare-feux, les réseaux, le cloud, les identités, les sauvegardes et les outils de productivité. • Vous souhaitez une corrélation plus rapide des menaces et une réduction de la surproduction d'alertes. • Vous souhaitez un meilleur ROI de vos investissements actuels et futurs dans les technologies informatiques et de cybersécurité.	• Vous ne surveillez que les terminaux et les serveurs. • Vous avez besoin d'un soutien opérationnel plus important que celui que votre équipe peut vous apporter. • Vous ne disposez pas des ressources internes nécessaires pour gérer une plateforme XDR.
MDR	• Vous avez besoin d'une détection et d'une réponse aux menaces assurées par des experts, 24 h/24 et 7 j/7. • Vous êtes confronté à une surproduction d'alertes, à une pénurie de personnel qualifié ou à un épuisement professionnel. • Vous recherchez un partenaire proactif pour investiguer et neutraliser les menaces en votre nom. • Vous souhaitez améliorer votre position en matière de cyberassurance, en vue de réduire les primes et d'augmenter la couverture.	• Vous êtes doté d'un SOC interne déjà bien établi, avec un personnel et des capacités adéquates, offrant une couverture 24/7/365 robuste. • Vous n'êtes pas encore prêt à externaliser certaines parties de vos opérations de détection et de réponse.

AUTRES ÉLÉMENTS À CONSIDÉRER AVANT TOUTE DÉCISION

Lorsque vous évaluez les différentes options, plusieurs facteurs essentiels peuvent déterminer si une solution EDR, XDR ou MDR est la mieux adaptée, et quel partenaire est en mesure de tenir cette promesse.

L'importance des renseignements sur les menaces

L'efficacité de toute solution de détection et de réponse dépend de la qualité des renseignements sur les menaces qui la sous-tendent. Plus les renseignements sont vastes, approfondis et récents, plus les menaces peuvent être repérées et neutralisées rapidement. Assurez-vous que tout fournisseur que vous envisagez de choisir est en mesure d'expliquer les sources et la portée de leurs données sur les menaces.

Un service doit être plus qu'une promesse

Même la meilleure technologie peut s'avérer insuffisante sans un support réactif. Que vous gériez vous-même vos services ou que vous fassiez appel à un partenaire pour des services managés, il est essentiel de savoir qu'une assistance est disponible lorsque vous en avez besoin. Demandez aux fournisseurs comment le support fonctionne concrètement : qui répond, à quelle vitesse, ce qui est inclus et comment obtenir de l'aide pendant un incident actif.

Le coût est parfois trompeur

Ne présumez pas qu'une option est intrinsèquement plus coûteuse qu'une autre. Les prix varient considérablement en fonction de la manière dont chaque solution est implémentée et prise en charge. Concentrez-vous sur vos besoins spécifiques et tenez compte de vos effectifs et de vos investissements actuels, y compris les compromis possibles entre les technologies et le coût des ressources internes par rapport aux ressources externalisées.

Les solutions de détection et de réponse, en particulier les services MDR, peuvent influencer les coûts de votre cyberassurance. De nombreux assureurs voient désormais d'un bon œil les organisations qui ont mis en place une surveillance et une réponse aux menaces 24/7, ce qui peut se traduire par une réduction des primes ou une amélioration des conditions de couverture.

Une analyse complète du ROI tenant compte des économies opérationnelles, de la réduction des risques et même des avantages en matière d'assurance peut vous aider à déterminer le véritable coût et la valeur de chaque approche.

EN CONCLUSION

1,53 million $

Le coût moyen pour se rétablir après une attaque de ransomware, sans compter le paiement d'une rançon.*

40 %

des organisations touchées par un ransomware indiquent qu'un manque d'expertise en cybersécurité a contribué à l'attaque.*

Les enjeux sont trop importants pour s'en remettre à des conjectures.

Choisir la bonne stratégie de détection et de réponse ne se résume pas à une question de technologie ; il s'agit également de responsabiliser vos collaborateurs, de protéger vos opérations et de mettre en place une cyberdéfense résiliente et durable.

*Rapport Sophos L'état des ransomwares en 2025

SOPHOS
DEFEAT CYBERATTACKS

OBTENEZ PLUS D'INFORMATIONS SUR LES SOLUTIONS ET SERVICES SOPHOS

Sophos vous aide à mieux détecter et répondre aux menaces aujourd'hui et à anticiper l'évolution de vos besoins de cybersécurité.

Contactez nos experts Sophos et déterminons ensemble la solution la mieux adaptée à votre activité.