Guide de l'acheteur

# Comprendre les outils XDR

## Qu'est-ce que l'XDR et comment cette technologie peut renforcer votre sécurité

Rene Holt

Digital Security
Progress. Protected.

Digital Security
**Progress. Protected.**



# Table des matières

# Introduction

Si vous êtes responsable de la sécurité informatique de votre entreprise, ce guide sur la détection et la réponse étendues (XDR) a deux objectifs.

- **Tout d'abord, comprendre comment l'XDR peut renforcer la sécurité de votre entreprise.**
- **Ensuite, il s'agit de souligner les fonctionnalités d'une solution d'XDR qui méritent d'être prises en compte dans votre décision d'achat.**

La question préalable à l'achat d'une solution d'XDR est la suivante : en avez-vous besoin ? De nombreux défis peuvent être à l'origine d'un tel besoin, qu'il s'agisse de l'augmentation des ransomwares, du risque d'attaques contre la chaîne d'approvisionnement, du détournement des outils d'administration informatique par les attaquants, ou encore des exigences réglementaires et des assurances.

Mais au-delà des menaces et des exigences, une multitude de messages marketing a brouillé le sens même de l'XDR. Selon une définition, une solution peut être considérée comme véritablement XDR, mais selon une autre, elle est seulement semblable à de l'XDR.

Est-il trop audacieux de dire que les fournisseurs définissent l'XDR en fonction des atouts particuliers de leurs solutions ? Ou faut-il plutôt dire que les fournisseurs conçoivent leurs solutions d'XDR selon des philosophies aussi différentes les unes des autres que leur expérience pratique en matière de sécurité ?

La question n'est pas de savoir quelle philosophie est la bonne ou la mauvaise, mais laquelle est la plus logique pour l'entreprise que vous êtes chargé de protéger, avec les ressources dont vous disposez.

Les fournisseurs ont le devoir d'exposer clairement leur philosophie afin que vous puissiez prendre une décision fondée sur une vision précise de l'XDR de chaque fournisseur. À la fin de ce guide, nous espérons vous avoir transmis au moins un message durable : notre solution d'XDR, ESET Inspect, redonne aux défenseurs d'une organisation le pouvoir de décision quant aux mesures de détection et de réponse à apporter.

ESET Inspect dote les administrateurs informatiques d'un outil suffisamment puissant pour recueillir les informations nécessaires à la prise de décisions en toute confiance. Les effets positifs cumulés pour vos défenses comprennent une meilleure évaluation des risques, une réduction des dépenses de sécurité à long terme, une simplification des processus de sécurité ainsi qu'une accélération de la détection, de l'investigation et de la réponse aux menaces.

La question n'est pas de savoir quelle philosophie est la bonne ou la mauvaise, mais laquelle est la plus logique pour l'entreprise que vous êtes chargé de protéger, avec les ressources dont vous disposez.

# Chapitre 1 : Menaces actuelles

## La cyberguerre entre défenseurs et adversaires est une lutte sans fin. De 2021 à 2022, la télémétrie d'ESET a enregistré une augmentation de 13 % du nombre total de détections de menaces.

Bien que la sécurité des endpoints soit une aide indispensable dans cette lutte, certaines menaces semblent défier même cette protection, en particulier lorsque des failles de sécurité béantes sont laissées sur des systèmes exposés.

Pour mieux comprendre comment l'XDR peut contribuer à lutter contre ces menaces dangereuses, examinons-en quatre : les ransomwares et les wipers, le détournement des outils d'administration informatique, les fuites de secrets d'entreprise et les attaques contre la chaîne d'approvisionnement. Bien que ces menaces ne soient pas les seules que l'XDR aide à combattre, elles représentent des défis qu'il peut être particulièrement difficile de relever sans elle.

### LE DÉCLIN DES RANSOMWARES ET L'ESSOR DES WIPERS

En 2022, la télémétrie d'ESET a enregistré une baisse des ransomwares et une augmentation des wipers, en particulier en Ukraine. Cette baisse est-elle due à la diminution des attaques de ransomwares ? Ou bien les attaques potentielles de ransomwares ont-elles été détectées plus tôt, empêchant les attaquants de déployer des ransomwares ?

Quelle que soit la réponse, les ransomwares et les wipers constituent une préoccupation majeure en raison des dommages catastrophiques qu'ils peuvent causer. Lorsque les opérateurs de malwares exfiltrent des données, ils peuvent même tenter une double pénalisation de la victime, en promettant de ne pas divulguer les données si les demandes sont satisfaites. Même si les chances sont faibles, les dommages potentiels sont suffisamment importants pour justifier un examen approfondi de vos défenses contre des malwares aussi destructeurs.

Une attaque suffisamment furtive pourrait exploiter une faille ou une faiblesse dans vos défenses, et tenter ensuite de déployer un ransomware ou un wiper, tout en échappant à la détection. L'XDR peut apporter aux défenseurs une visibilité sur les premières (et les dernières) étapes d'une attaque, les aidant ainsi à détecter l'attaque dès les premiers stades avant toute tentative de déploiement de malwares destructeurs. En d'autres termes, en utilisant l'XDR pour la recherche de menaces, vous pouvez réduire considérablement le temps de présence des adversaires dans votre réseau.

### DÉTOURNEMENT DES OUTILS D'ADMINISTRATION INFORMATIQUE

Les attaquants sont tout aussi versés dans l'utilisation des outils d'administration informatique que les défenseurs, ce qui signifie que le détournement de ces outils peut fournir une fausse impression de légitimité. PowerShell, certutil, PsExec et SDelete font partie des outils employés par les attaquants.

Par exemple, LookingFrog, un groupe d'adversaires connu pour cibler des missions diplomatiques, des organisations caritatives et des entreprises de fabrication industrielle, a utilisé le logiciel certutil pour implémenter un shell web. Agrius, connu pour cibler des entreprises de ressources humaines, des sociétés de conseil en informatique, des grossistes en diamants et des bijoutiers, a utilisé PsExec pour déployer le wiper Fantasy via un fichier batch Windows. NikoWiper, basé sur l'outil SDelete permettant de supprimer des fichiers en toute sécurité, a été détecté dans une entreprise ukrainienne du secteur de l'énergie.

Les outils utilisés par les administrateurs informatiques possèdent des fonctionnalités qui, entre de mauvaises mains, peuvent être utilisées pour télécharger des malwares, reconfigurer des systèmes, désactiver des paramètres de sécurité, effectuer de la reconnaissance et même détruire des données. Comme ces outils sont légitimes, les logiciels de sécurité des endpoints sont limités dans leur capacité à différencier l'usage légitime du détournement.

Cependant, avec l'XDR, vous pouvez surveiller la façon dont les outils d'administration informatique sont utilisés et alerter les défenseurs sur des actions qui ne sont pas typiques des administrateurs ou qui sont potentiellement dangereuses.

### FUITES DE SECRETS D'ENTREPRISE

Lors d'une découverte inattendue par des chercheurs d'ESET, un certain nombre de routeurs centraux provenant du marché de l'occasion contenaient des informations sensibles liées à leur ancienne utilisation dans des réseaux d'entreprise. Ce résultat est surprenant, car on pourrait penser que les grandes entreprises disposent des procédures et du personnel nécessaires pour veiller à ce que les appareils soient correctement effacés avant d'être revendus.

Étant donné que ces appareils sont peu coûteux pour les pirates, toute donnée sensible qui y est laissée pourrait donner un coup de pouce aux plans d'intrusion dans ces réseaux.

Face à de telles fuites, deux mesures au moins peuvent être prises. Tout d'abord, cessez d'utiliser toutes les clés cryptographiques qui ont pu être stockées sur des appareils revendus, afin qu'elles ne puissent pas être exploitées pour obtenir un accès non autorisé à votre réseau. Deuxièmement, intégrez l'XDR pour traquer les attaquants qui exploitent les secrets d'entreprise de votre réseau.

### ATTAQUES CONTRE LA CHAÎNE D'APPROVISIONNEMENT ET RISQUES POUR LES TIERS

Naturellement, les entreprises font confiance à leurs fournisseurs de logiciels pour veiller à ce que les mises à jour ne sont pas infectées par des chevaux de Troie. Les attaquants qui compromettent les développeurs de logiciels peuvent abuser de cette confiance pour obtenir un accès initial aux environnements des clients.

Dans une campagne Agrius par exemple, les serveurs de mise à jour d'un développeur israélien de logiciels pour le secteur du diamant ont été compromis et utilisés pour envoyer aux clients une mise à jour malveillante contenant le wiper Fantasy.

Étonnamment dans une campagne Tick, les attaquants ont compromis les serveurs de mise à jour d'une société de prévention

[1] Plus d'informations dans le Rapport d'ESET sur les menaces au T3 2022.

des pertes de données afin de se déplacer latéralement sur le réseau, plutôt que d'attaquer des clients externes via la chaîne d'approvisionnement.

Autre rebondissement dans cette campagne Tick, des programmes d'installation pour Q-Dir, un explorateur de fichiers à plusieurs volets pour Windows, ont été infectés par un cheval de Troie et transférés via des outils d'assistance à distance aux clients de l'entreprise compromise, probablement au cours de sessions d'assistance technique.

L'XDR est pertinente pour les menaces de ce type car elle peut alerter les défenseurs d'une activité malveillante suite à l'exploitation d'une relation de confiance avec un fournisseur de logiciels ou un autre tiers.

Les ransomwares et les wipers constituent une préoccupation majeure en raison des dommages catastrophiques qu'ils peuvent causer. Lorsque les opérateurs de malwares exfiltrent des données, ils peuvent même tenter une double pénalisation de la victime, en promettant de ne pas divulguer les données si les demandes sont satisfaites.



# Chapitre 2 : Qu'est-ce que l'XDR ?

Après avoir examiné certaines des menaces aux quelles sont confrontées les organisations et le rôle de l'XDR dans la détection de ces menaces, jetons un coup d'œil rapide au marché de l'XDR.

## PRÉVISIONS DU MARCHÉ

Selon Gartner, moins de 5 % des organisations utilisaient l'XDR en 2022, mais plus de 40 % d'entre elles devraient l'utiliser d'ici la fin de 2027. Il s'agit d'une croissance incroyable dans l'adoption de l'XDR ! Un autre cabinet d'analyse, IDC, prévoit une croissance tout aussi incroyable, mais en termes de revenus. Un rapport d'IDC de mars 2022 prévoyait que le chiffre d'affaires mondial de l'XDR dans le Cloud connaîtrait un taux de croissance annuel composé de 69,5 % entre 2021 et 2026.

Alors que les organisations cherchent à améliorer leurs atouts face aux adversaires, l'XDR s'est clairement imposée comme une solution de choix.

## DÉFINITION DES TERMES

Comme nous l'avons mentionné dans l'introduction, les fournisseurs définissent différemment l'XDR et les termes connexes tels que la détection et la réponse pour endpoints (EDR) et la détection et la réponse managées (MDR). Même la frontière entre la sécurité des endpoints et l'EDR semble parfois floue dans les documents marketing. En raison de la confusion autour de ces termes, il n'est pas rare que des critiques fondées sur des définitions, des attentes et des expériences différentes soient exprimées. Cette confusion est probablement due au fait que de nombreux fournisseurs abordent l'XDR à partir de différents domaines d'expertise. Pour ESET, l'aventure a commencé il y a plus de trente ans avec l'étude des malwares et le développement de logiciels de sécurité pour endpoints, qui ont ensuite débouché sur l'EDR, et maintenant l'XDR. D'autres fournisseurs peuvent approcher l'XDR avec une expérience dans l'analyse de la sécurité ou des plateformes de renseignement sur les menaces.

Nous allons ici donner une explication rapide et basique de la façon dont ESET comprend ces termes.

## EDR VERSUS SÉCURITÉ DES ENDPOINTS

Pour protéger les appareils, la sécurité des endpoints utilise plusieurs couches de technologie, chacune d'entre elles étant conçue pour détecter et bloquer automatiquement les menaces. Pour l'administrateur informatique, la sécurité des endpoints est largement automatisée. D'une certaine manière, cela est bénéfique car l'administrateur informatique n'est pas accablé par les problèmes de sécurité qui sont traités immédiatement.

Mais l'administrateur informatique reçoit généralement peu d'informations sur la raison pour laquelle certaines menaces sont détectées, c'est-à-dire que la cause

sous-jacente plus profonde aux symptômes détectés n'est pas fournie. Une solution d'EDR donne à l'administrateur informatique une visibilité sur les événements qui se produisent sur les endpoints, ce qui permet de diagnostiquer les symptômes.

Une solution d'EDR peut détecter des événements spécifiques, ou des séquences d'événements, qui sont suspects ou qui méritent d'être surveillés. Ces détections sont déclenchées par un moteur qui analyse ces événements et alerte l'administrateur lorsqu'une correspondance se produit niveau du comportement. L'EDR met également à la disposition des administrateurs des actions de réponse, telles que l'arrêt d'un processus, l'isolement d'un ordinateur du réseau, le blocage d'un exécutable, etc.

En bref, l'EDR exige une approche pratique et active de la sécurité car elle permet aux défenseurs de surveiller et d'enquêter sur des événements de bas niveau qui pourraient s'avérer être des techniques d'attaque. D'autres mesures proactives, telles que la simulation des adversaires et la recherche de menaces, deviennent également plus faciles à mettre en œuvre grâce à l'EDR.

## Qu'est-ce que l'EDR ?

Une technologie de détection, d'investigation et de réponse qui collecte des données télémétriques sur la sécurité à partir des endpoints, détecte des anomalies, permet aux analystes d'enquêter à partir des données télémétriques collectées, et facilite la réponse des analystes sur les endpoints concernés.

Source : *Forrester, 2021*

## XDR VERSUS EDR

Si une solution d'EDR peut ingérer des données provenant d'appareils et de sources supplémentaires, tels que des appareils réseau et des services dans le Cloud, il s'agit alors d'une solution d'XDR. Le terme « étendues » fait référence ici aux données au-delà des endpoints. L'évolution de l'EDR vers l'XDR nécessite une intégration accrue avec les solutions de sécurité du fournisseur et, éventuellement, de tiers.

L'un des défis qui stimule la croissance de l'XDR est la lassitude causée par une multiplicité d'outils qui ne fournissent qu'une visibilité fragmentaire sur la sécurité d'une organisation. Lorsque davantage de types de données peuvent être introduits dans un moteur de détection et fournis au défenseur d'une manière convaincante et facile à comprendre, il obtient alors une visibilité plus étendue sur la sécurité de l'organisation. En retour, cela peut conduire à une réponse plus efficace aux incidents et une automatisation accrue.

Toutefois, l'obtention de cette vue d'ensemble n'est pas toujours bénéfique pour la recherche de menaces quand les données proviennent de l'extérieur. Les sources de données du fournisseur étant généralement plus riches et mieux normalisées que les données de tiers, une intégration accrue avec les solutions du fournisseur (également appelée XDR native) permet généralement de mieux repérer les attaques et d'y répondre.



## XDR VERSUS EDR

Étant donné que l'XDR est plus efficace lorsqu'elle est managée par un personnel hautement qualifié qui y consacre du temps, l'externalisation de la gestion de l'XDR peut être une option souhaitable. Comme son nom l'indique, le MDR est un service de sécurité managé qui associe l'XDR à des experts en cybersécurité et des services supplémentaires proposés par le fournisseur ou un tiers. Certains utilisent même le terme MxDR pour se différencier de l'« ancienne » signification du MDR qui se référait à l'EDR.

Le MDR peut aider les organisations à surmonter certaines difficultés pour passer à l'XDR, ce qui ne serait pas possible autrement. Ces défis comprennent la lassitude face aux alertes, la difficulté à recruter du personnel de sécurité talentueux ou expérimenté, les coûts de fonctionnement d'un centre d'opérations de sécurité interne, et le temps nécessaire pour faire face à l'évolution rapide des menaces.

## Qu'est-ce que l'XDR ?

L'XDR est une évolution de l'EDR, qui optimise la détection, l'investigation, la réponse et la recherche de menaces en temps réel. L'XDR unifie les détections pertinentes pour la sécurité sur les endpoints avec la télémétrie des outils de sécurité et d'entreprise, tels que l'analyse et la visibilité sur le réseau (NAV), la sécurité de la messagerie, la gestion des identités et des accès, la sécurité du Cloud, etc. Il s'agit d'une plateforme native dans le Cloud reposant sur une infrastructure de big data pour fournir aux équipes de sécurité de la flexibilité, de l'évolutivité et des possibilités d'automatisation.

Source : *Forrester, 2021*

### Problèmes éventuels liés aux fonctionnalités de l'XDR

# Chapitre 3 : Comment l'XDR peut vous aider ?

Si la surveillance des événements de bas niveau sur les endpoints peut sembler intéressante pour les analystes de la sécurité, prenons un peu de recul et considérons les avantages pour la sécurité de votre entreprise. La détection d'événements suspects peut-elle réellement améliorer vos défenses ?

## AVANTAGES CLÉS

Les organisations qui utilisent l'XDR pour la première fois peuvent être surprises par la quantité d'événements qui déclenchent des détections. Il peut s'agir d'un moment décisif qui révèle une multitude de systèmes mal configurés, de vulnérabilités ou de menaces. Le déploiement initial de l'XDR peut donc rapidement déboucher sur deux avantages : la mise au jour de mauvaises pratiques de cyber-hygiène au sein de votre organisation et la découverte des menaces qui se cachent dans votre réseau.

Au chapitre 1, nous avons examiné un certain nombre de menaces contre lesquelles les organisations pourraient avoir des difficultés à se défendre sans l'XDR, ce qui signifie qu'avec l'XDR, vous bénéficiez des avantages suivants : une meilleure confiance dans la détection des ransomwares, des wipers et des attaques contre la chaîne d'approvisionnement, et dans la découverte des attaquants qui détournent des outils d'administration informatique ou qui exploitent les secrets de l'entreprise, peut-être dérobés sur des appareils mis hors service.

En raison de la visibilité accordée aux événements de bas niveau, un autre avantage de l'XDR est que les défenseurs peuvent tester leur couverture des tactiques et techniques adverses décrites dans la Base de connaissances MITRE ATT&CK®. Bien entendu, il existe souvent plusieurs façons de mettre en œuvre une technique, qui ne sont pas toutes enregistrées dans ATT&CK. Cependant, les techniques enregistrées servent de repères fidèles sur le chemin de la découverte des faiblesses et des lacunes de vos défenses. Pour faciliter l'imitation des adversaires, les solutions d'XDR renvoient les détections aux techniques ATT&CK.

Un autre avantage de l'XDR est la recherche de menaces. Les actualités sur la sécurité révèlent souvent des attaques en cours, qui se produisent parfois à grande échelle. Les défenseurs se précipitent sur leurs consoles pour tester les nouvelles attaques signalées et adapter leurs défenses en conséquence. L'XDR offre l'avantage de pouvoir rédiger des règles de recherche de menaces capables de rechercher dans votre base de données des événements signalant potentiellement des compromissions.

Une fois la menace découverte, l'XDR propose différentes options de remédiation au personnel chargé de répondre à l'incident. Pour réduire le délai moyen de réponse aux menaces, l'XDR peut déclencher des actions automatiquement.

Le personnel chargé de répondre aux incidents s'intéresse également à la possibilité de retracer les attaques jusqu'à l'accès initial. Étant donné que l'XDR suit les arborescences de processus et peut corréler les événements, les intervenants sont mieux placés pour découvrir le vecteur d'attaque initial. Cette possibilité est particulièrement cruciale pour atténuer les attaques qui commencent par l'exploitation d'une vulnérabilité zero-day ou non encore corrigée, les attaques contre la chaîne d'approvisionnement et les menaces internes.

L'XDR facilite également la coopération entre les intervenants en cas d'incident, en intégrant des fonctions de collaboration inspirées des plateformes de réponse aux incidents.

### Démontrer la valeur de l'XDR

En 2023 et au-delà, IDC prévoit que les fournisseurs passeront de la promotion de leur préparation à l'XDR à la démonstration de preuves tangibles de la valeur multiforme de l'XDR. Cette démonstration de valeur comprend les éléments suivants : une meilleure compréhension par les organisations des cyber-risques et des moyens de réduire structurellement ces risques, l'amélioration des mesures de performance (par ex. le temps moyen de détection, d'investigation et de réponse) et la réduction de l'impact de la prolifération des technologies de cybersécurité sur les dépenses globales de sécurité des organisations et sur la complexité collective.

Source : *IDC, Worldwide Modern Endpoint Security Market Shares, juillet 2021–juin 2022 : Currency Exchange Rates Slightly Trimmed Accelerating Growth, Doc # US49982022, janvier 2023*

# Chapitre 4 : Ce qu'il faut rechercher en matière d'XDR

Ce chapitre présente aux acheteurs potentiels de solutions XDR les neuf critères qu'ils doivent prendreen compte avant d'acheter.

### DÉTECTION

Pour détecter les attaques, l'XDR surveille les événements. Certains événements peuvent, selon les circonstances, être le signe d'une intention malveillante ou d'une simple activité bénigne. Ce double objectif augmente le risque de faux positifs. Par conséquent, une solution d'XDR devrait intégrer un moteur de détection qui a été bien testé dans sa configuration par défaut afin de minimiser les faux positifs pour le plus grand nombre possible d'organisations.

La stratégie adoptée par l'XDR pour minimiser les faux positifs implique un équilibre délicat. Il est parfois préférable, dans un environnement particulier, de ne pas activer de règles d'XDR pour les événements fréquemment générés et observés dans les attaques, mais de s'appuyer sur la détection de l'attaque par un autre événement. L'attaque est toujours détectée, même si vous n'avez pas été alerté à chaque étape. Cela signifie que toutes les solutions d'XDR ne surveillent pas nécessairement les mêmes événements pour détecter la même attaque.

Autre complication : la fréquence d'un événement est influencée par l'utilisation de systèmes, d'applications ou d'outils particuliers au sein d'une organisation. Ce qui est courant pour une organisation peut ne pas l'être pour une autre. Il en va de même pour les fonctions au sein d'une entreprise.

Une autre considération est qu'un trop grand nombre de détections de faux positifs entraîne une lassitude des administrateurs, ce qui nécessite l'optimisation de la solution d'XDR après le déploiement initial. Si votre organisation n'est pas en mesure d'effectuer l'optimisation initiale, recherchez un fournisseur d'XDR qui propose ce service.

Toute détection doit inclure un contexte, comme les causes malveillantes et bénignes possibles, une estimation de la gravité et des informations sur les événements qui l'ont déclenchée. Après tout, l'XDR est conçue pour faciliter le travail d'investigation des chasseurs de menaces.

Enfin, il convient d'examiner les sources de détection, qui ont une incidence déterminante sur la capacité d'une solution d'XDR à détecter les menaces. Les données télémétriques comprennent-elles des détections provenant de la surveillance des API, de l'analyse de la mémoire, des scripts exposés par Windows Antimalware Scan Interface (AMSI), ou même de l'analyse du contenu du trafic réseau ? Pour des raisons de robustesse, les sources de détection devraient se chevaucher.



### RÉPONSE

L'XDR devrait proposer des étapes d'investigation recommandées, des actions de remédiation et une réponse automatisée. Ces actions peuvent consister à bloquer le lancement d'exécutables et le chargement de bibliothèques de code (DLL), arrêter ou redémarrer l'ordinateur, forcer la déconnexion, isoler l'ordinateur, terminer les processus et nettoyer les fichiers.

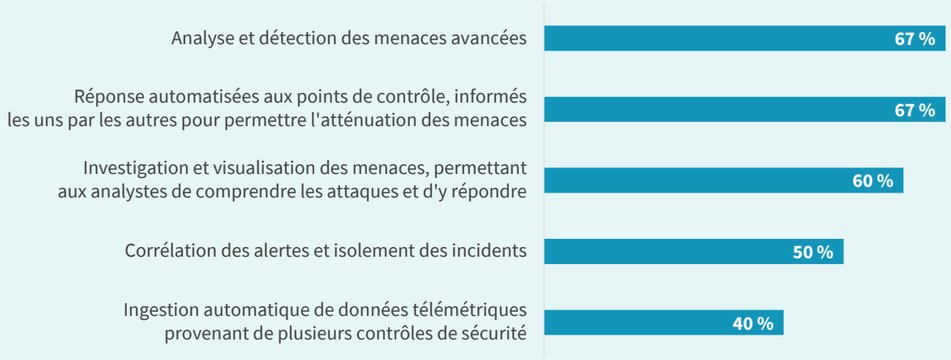
Les acheteurs potentiels devraient se méfier des réponses automatisées trop agressives qui perturbent le fonctionnement des systèmes dans leur environnement. Une partie des tests sur les faux positifs pour une nouvelle règle devrait inclure une évaluation de la gravité de la menace associée à la détection, et de la probabilité que la cause soit malveillante, avant d'y associer des réponses automatisées qui bloquent l'exécution ou terminent un processus.

Dans une enquête de 2022 auprès de grandes entreprises et d'entreprises de taille moyenne en Amérique du Nord, les professionnels de la cybersécurité ont identifié la détection et la réponse comme étant les fonctionnalités XDR les plus critiques. (Voir le graphique à la page suivante.)

## L'XDR surveille les événements de faible niveau, notamment :

- Requêtes HTTP
- Connexions TCP/IP
- Injection requestsCode DNS
- Valeurs définies dans la base de registre
- Clés supprimées de la base de registre
- Opérations sur les fichiers
- Appels à l'API Windows
- Événements WMI
- Scripts
- Chargement de DLL
- Chargement de pilote
- Chargement de module du noyau
- Exécutables abandonnés
- Création d'un tuyau nommé
- Événements liés au compte utilisateur
- Détection de sécurité sur les endpoints

**Quelles sont les fonctionnalités les plus critiques qu'une solution XDR doit fournir avant que votre organisation n'envisage de mettre hors service sa solution EDR ? (Pourcentage des répondants, N=329, réponses multiples acceptées)**




Source : *ESG Brief: The Demise of EDR?, avril 2022, p. 2.*

## ÉQUILIBRE

Bien qu'une visibilité accrue sur les événements puisse vous permettre de détecter davantage d'étapes d'une attaque, cela peut être une arme à double tranchant. Vous devez en voir suffisamment pour stopper une attaque, mais pas trop pour ne pas être submergé par les détections déclenchées par le comportement normal de votre organisation.

Le rôle d'une solution d'XDR équilibrée n'est pas d'alerter les défenseurs sur chaque procédure effectuée au cours d'une attaque, mais plutôt de les avertir qu'une attaque est en cours et de les aider à enquêter sur celle-ci.

## TRANSPARENCE

Certains fournisseurs de solutions d'XDR ferment leur moteur, de sorte que les administrateurs informatiques n'ont que peu ou pas de visibilité sur ce que la solution surveille. Même si toutes les organisations n'en ont pas l'utilité, un ensemble de règles ouvertes permet à l'analyste de sécurité de consulter, d'auditer et d'analyser les événements surveillés par la solution d'XDR.

## PERSONNALISATION

L'un des défis de la détection est celui des faux positifs. Mais lorsque l'ensemble des règles d'XDR est transparent, les administrateurs informatiques peuvent adapter la solution à leur environnement, ce qui réduit le nombre de faux positifs.

La personnalisation est au cœur de l'optimisation d'une solution d'XDR au départ comme par la suite. Envisagez une solution d'XDR qui vous permette de définir des exclusions personnalisées, modifier les réponses automatiques avec différentes actions et rédiger vos propres règles. Cela permet d'utiliser la solution de manière optimale, en fonction de ce qui est « normal » dans votre environnement.

En fin de compte, ce sont les défenseurs de l'organisation qui sont les mieux placés pour connaître la configuration du moteur d'XDR qui permet d'atteindre l'équilibre souhaité entre le risque et le bruit.



## INTÉGRATION

Une solution capable de s'intégrer aux solutions de sécurité du fournisseur et à celles de tiers est crucial pour l'XDR. L'intégration comprend l'exportation et l'importation de données dans l'outil d'XDR, par exemple via une API. Vérifiez si vous pouvez exporter des détections pour les utiliser dans un système de gestion des informations et des événements de sécurité (SIEM) et importer des hachages à partir de flux de données sur les menaces.

En ce qui concerne les intégrations natives, de nombreux fournisseurs proposent généralement des systèmes de sécurité des endpoints et des systèmes de réputation et de détection dans le Cloud qui, ensemble, fournissent des moyens complets de prévention, de détection et de réponse.

La technologie XDR s'appuie sur la protection offerte par la sécurité des endpoints et d'autres solutions. Il ne s'agit pas d'une technologie isolée. Il faut donc garder à l'esprit que la qualité des données de télémétrie générées par les solutions des différents fournisseurs varie. Les menaces bloquées par votre logiciel de sécurité des endpoints peuvent être un déclencheur pour approfondir les causes possibles avec l'XDR et rechercher des moyens d'améliorer les défenses.

## MULTIPLATEFORME

Côté client, l'XDR devrait prendre en charge les endpoints fonctionnant sous les principaux systèmes d'exploitation, tels que Windows, macOS et Linux. Grâce à la prise en charge multiplateforme, les défenseurs peuvent plus facilement suivre les mouvements latéraux des attaquants.

Côté serveur, l'achat et la maintenance du matériel et des logiciels nécessaires au serveur et à la base de données XDR sont des coûts potentiellement prohibitifs associés à l'XDR. Le matériel doit pouvoir gérer le nombre typique d'événements générés par tous les endpoints de votre organisation. Par ailleurs, si vous souhaitez une meilleure visibilité, cela peut augmenter le coût du matériel, car le stockage d'un grand nombre d'événements (en particulier ceux qui sont générés fréquemment) peut rapidement devenir une source d'accaparement des ressources.

Si le déploiement sur site n'est pas envisageable pour vous, optez pour une solution d'XDR dans le Cloud en confiant au fournisseur la responsabilité du matériel côté serveur.

## SERVICES

L'investissement dans l'XDR devrait aller au-delà du produit : il devrait inclure des services. Déterminez si le fournisseur propose les éléments suivants :

- Services de déploiement et d'optimisation
- Services de détection et de réponse managés, y compris la recherche de menaces
- Contrôles de l'état de la sécurité
- Un partenaire ou un bureau local dans votre région
- Support technique dans les langues locales

**PRESTATAIRE**
La valeur à long terme de votre investissement dans l'XDR dépend fortement de la stabilité et de la réputation du fournisseur. Tenez compte de l'expertise et des antécédents du fournisseur en matière de sécurité. Il s'agit notamment de l'ensemble du portefeuille de produits et de services du fournisseur, de ses compétences avérées en matière de prévention des menaces, de ses renseignements sur les menaces et des études publiées sur les malwares.

Examinez également les évaluations de tiers, telles que le Test EPR (Endpoint Prevention & Response) d'AV-Comparatives. Ce test évalue la réponse d'une solution d'XDR à de multiples scénarios d'attaque, sur un ensemble de trois phases : implantation initiale, propagation et atteinte à la sécurité des ressources.

MITRE Engenuity ATT&CK® Evaluations est une autre ressource qui compare les solutions d'XDR à des techniques adverses connues. Ces évaluations révèlent le niveau de visibilité sur les techniques malveillantes et la profondeur du contexte fourni par chaque détection. Il convient de souligner que ces évaluations n'ont pas de vainqueurs et qu'elles ne testent pas les faux positifs ni l'impact sur les performances.

Avec une solution d'XDR, vous pouvez bénéficier des avantages suivants : une confiance accrue dans la détection des ransomwares, des wipers et des attaques contre la chaîne d'approvisionnement, la découverte d'attaquants détournant des outils d'administration informatique ou exploitant les secrets de l'entreprise, peut-être dérobés sur des appareils mis hors service.



# Chapitre 5 : Comment ESET peut vous aider avec l'XDR

L'utilisation de l'analyse comportementale sur l'ensemble des endpoints, du réseau, du Cloud, de la messagerie et d'autres couches est un cadre définissant l'approche et la méthodologie d'ESET.

Elle permet de repérer les activités suspectes et de stopper les attaquants avant qu'ils n'aient un impact. Pour ce faire, ESET s'appuie sur ses solutions technologiques de pointe telles que l'XDR.

ESET Inspect, notre **solution d'XDR**, offre aux gestionnaires de risques et au personnel chargé de répondre aux incidents une visibilité exceptionnelle sur les menaces. Il leur permet d'effectuer une analyse rapide et approfondie des causes profondes, et de répondre immédiatement aux incidents. Associé à la puissance préventive éprouvée des produits de protection d'ESET pour endpoints, ESET Inspect est une solution d'XDR **dans le Cloud** capable de :

- Détecter les menaces persistantes avancées
- Bloquer les attaques sans fichiers
- Bloquer les menaces zero-day
- Protéger contre les ransomwares
- Empêcher les violations de la politique de sécurité de l'entreprise

## LA DIFFÉRENCE ESET

### PRÉVENTION, DÉTECTION ET RÉPONSE COMPLÈTES

ESET Inspect analyse et remédie rapidement à tout problème de sécurité dans votre réseau. La sécurité multicouche sous-jacente d'ESET, dans laquelle chaque couche envoie des données à ESET Inspect, analyse de grandes quantités de données en temps réel afin qu'aucune menace ne passe inaperçue.

### SOLUTION D'UN FOURNISSEUR PRIVILÉGIANT LA SÉCURITÉ

ESET lutte contre les cybermenaces depuis plus de 35 ans. En tant qu'entreprise à vocation scientifique, elle est depuis longtemps à la pointe du développement de technologies autours du machine learning, du Cloud, et maintenant de l'XDR.

### MIEUX VAUT PRÉVENIR QUE GUÉRIR

L'approche d'ESET en matière d'XDR est étroitement liée à ses produits de prévention primés. Grâce à notre engagement à développer une technologie de détection de haute qualité,

La technologie de prévention d'ESET est l'une des meilleures au monde.

### VISIBILITÉ DÉTAILLÉE SUR LE RÉSEAU

Avec des règles de détection transparentes (ESET en compte plus de 1250), des indicateurs de compromis (IoC) avancés et une fonctionnalité de recherche, un examen approfondi des exécutables fonctionnant sur votre réseau vous permettra d'identifier tout ce qui est suspect.

### PRÊT À L'EMPLOI IMMÉDIATEMENT

La solution d'ESET est prête à l'emploi dès son installation, et est suffisamment puissante pour être configurée de façon granulaire par les équipes expérimentées de recherche de menaces.

### FLEXIBILITÉ DU DÉPLOIEMENT

Nous vous laissons décider de la manière de déployer votre solution de sécurité : ESET Inspect peut être hébergé sur vos propres serveurs sur site ou dans le Cloud, ce qui vous permet d'adapter votre configuration en fonction de vos objectifs de coût total de possession et de vos moyens matériels.

### MITRE ATT&CK®

Les détections d'ESET Inspect s'appuient sur le cadre MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge), qui fournit des informations complètes en un clic, même sur les menaces les plus complexes. ESET est l'un des principaux éditeurs indépendants de logiciels de cybersécurité et figure dans le top 10 des 350 contributeurs d'ATT&CK.

### SYSTÈME DE RÉPUTATION

Le filtrage étendu permet aux ingénieurs en sécurité d'identifier toutes les applications connues à l'aide du système robuste de réputation d'ESET. Le système d'ESET intègre une base de données de centaines de millions de fichiers bénins afin de garantir que les équipes de sécurité puissent se consacrer à des fichiers inconnus, et potentiellement malveillants, et non sur des faux positifs.

### AUTOMATISATION ET ORCHESTRATION

Adaptez facilement ESET Inspect au niveau de détail et d'automatisation dont vous avez besoin. Choisissez le niveau d'interaction souhaité, ainsi que le type et la quantité de données à stocker, lors de la configuration initiale et à l'aide de profils d'utilisateurs prédéfinis, puis laissez le mode apprentissage cartographier l'environnement de votre entreprise et suggérer au besoin des exclusions pour les faux positifs.

## AVANTAGES DE LA SOLUTION D'XDR D'ESET

Les entreprises ont désormais besoin d'une plus grande visibilité sur les endpoints, les appareils et les réseaux pour protéger leurs profits et leur réputation contre les menaces émergentes, les risques sur les collaborateurs et les applications indésirables. **ESET Inspect**, qui fait partie d'ESET PROTECT, est **une solution d'XDR dans le Cloud** qui offre une détection unique basée sur la réputation et les comportements, avec un feedback en temps réel pour les équipes de sécurité à l'aide de renseignements sur les menaces globales issus d'ESET LiveGrid®. Les organisations peuvent bénéficier de cette solution grâce à :



### EXPERTISE

Détection et réponse d'un fournisseur de confiance, basé sur la recherche et privilégiant la sécurité, avec plus de 35 ans d'expérience à la pointe de la cybersécurité.

### QUALITÉ

Intégration étroite avec les produits de prévention multicouches d'ESET, basés sur une technologie primée et reconnue par l'ensemble du secteur.

### FLEXIBILITÉ

Solution prête à l'emploi et suffisamment puissante pour les chasseurs de menaces expérimentés. Elle offre des contrôles granulaires pour une adaptation optimale à l'environnement de chaque utilisateur.

### TRANSPARENCE

Des règles de détection transparentes garantissent une visibilité détaillée sur plusieurs couches, y compris la messagerie, les réseaux et les serveurs.

L'approche et la méthodologie d'ESET permettent de repérer les activités suspectes et de stopper les attaquants avant qu'ils n'aient un impact. Pour ce faire, ESET s'appuie sur ses solutions technologiques de pointe telles que l'XDR.

# Déploiement de l'XDR : scénario en conditions réelles

## Le client

**Le groupe Raicam** est une entreprise automobile spécialisée dans la conception, le développement et la production de freins, d'embrayages et de vérins. Raicam accorde une grande importance à la qualité et la sécurité des produits et des services de son portefeuille. De nombreux constructeurs automobiles parmi les plus connus au monde ont choisi de travailler avec Raicam en raison de la qualité de ses produits.

## Le défi

Avec plusieurs bureaux internationaux, Raicam avait besoin d'une solution de cybersécurité capable d'offrir une couverture complète au niveau mondial, un système facile à gérer mais garantissant un niveau élevé de protection contre les cyber-risques. Un autre facteur qui a conduit Raicam à envisager une nouvelle solution était la nécessité de disposer d'un produit de protection des endpoints doté de la **technologie XDR**, facile à intégrer et peu gourmand en ressources. L'objectif : un contrôle centralisé à partir d'une console unique permettant de gérer tous les contrôles de sécurité sans travail supplémentaire pour les équipes internes.

## La solution

Raicam a confié à **ESET** la sécurité informatique de ses différents sites de production en Italie et à l'étranger. Le groupe a adopté la Plateforme ESET PROTECT qui intègre différentes solutions dans une console d'administration unique, notamment ESET Inspect, **la solution d'XDR**.

Grâce à ce cadre de cybersécurité complet, les endpoints et les serveurs de Raicam sont protégés contre les attaques de ransomware, les menaces zero-day, les atteintes à la sécurité des données et plus encore, assurant ainsi la continuité des activités et la sauvegarde des données critiques de l'entreprise. Le tout avec un support client étendu, disponible 24h/24. L'adoption d'une technologie aussi robuste a également aidé Raicam à satisfaire aux normes réglementaires.


« L'approche multicouche d'ESET en matière de sécurité nous permet de répondre positivement aux audits de sécurité demandés par nos clients. »

Antonella Bertola, IS Manager chez Raicam

# Qu’est-ce que le MDR ?

Il s’agit d’un type de **service de sécurité managé** qui combine des outils, des technologies et des experts en cybersécurité pour fournir aux entreprises des moyens robustes de détection et de réponse.

Le MDR est effectivement une version externalisée de la détection et de la réponse étendues (XDR), parfois combiné à d’autres outils.

« Les services de MDR couvrent déjà une grande partie de ce que l’XDR aspire à faire. Le MDR permet d’obtenir de meilleurs résultats de sécurité en fournissant des outils et des technologies tels que les renseignements sur les menaces, la recherche de menaces, la surveillance constante 24 h/24, l’analyse avancée, ainsi que le confinement et l’élimination des brèches ou des incidents par lesquels des données ont été exfiltrées ou détruites.

Source : IDC Global Security Products Analysis: From PowerPoint to Power Product, Where Is XDR Right Now, doc. n° US47705821, 8 février 2022, Ch. Kissel, M. Suby, F. Dickson

# Qu’est-ce qu’**ESET PROTECT MDR** ?

La solution prend en charge la gestion des cyber-risques en offrant une visibilité sur votre environnement informatique, géré à partir d’une console unique qui peut être installée sur site ou dans le Cloud, en fonction de vos besoins. Le service ESET MDR est une solution holistique qui peut être achetée dans le cadre de l’offre ESET PROTECT MDR. Il s’agit d’une option plus complète combinant des produits et des services de prévention, de détection et de réponse.

## ESET, LEADER DU MDR EN 2023

**KuppingerCole** compare les fournisseurs de MDR sur la base de critères standardisés dans les catégories Produit, Innovation et Position sur le marché. Son rapport met en évidence les leaders globaux parmi les fournisseurs de MDR, et **ESET** est fière d’être reconnue à la fois comme un **leader du marché** et comme un **leader global** dans le 2023 MDR Leadership Compass grâce à ESET PROTECT MDR.



# Conclusion

L’XDR n’est pas isolée du reste des défenses d’une organisation. L’XDR joue plutôt son meilleur rôle au sein d’un écosystème de sécurité proactif qui comprend une protection moderne des endpoints, le sandboxing dans le Cloud, le machine learning, les renseignements sur les menaces et un personnel de sécurité dédié.

Cette approche multicouche de la sécurité est cruciale car, s’il est important d’avoir une meilleure visibilité sur une attaque se produisant sur votre réseau, il est encore plus important de pouvoir passer au crible une myriade d’événements pour repérer une attaque. Vous pouvez alors passer plus rapidement aux étapes de remédiation, en empêchant l’attaque de continuer à progresser.

Bien entendu, il est préférable de bloquer une attaque dès la première tentative d’accès, ou du moins peu de temps après. Vous pouvez y parvenir en prenant le temps de tester vos défenses de manière approfondie contre les techniques adverses avec l’XDR à vos côtés.

# À propos d'ESET

## Quand la technologie engendre le **progrès**, ESET est là pour **le protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

**protégé par ESET depuis 2016**
plus de 32 000 endpoints

T··

**partenaire FAI depuis 2008**
2 millions d'utilisateurs

Allianz Suisse

**protégé par ESET depuis 2016**
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

**protégé par ESET depuis 2017**
plus de 9 000 endpoints

**+ 30**
années d'expertise

**+ 1 Mrd**
d'internautes protégés

**+ 400 k**
entreprises clientes

**195**
pays et territoires

**13**
centres de recherche

**Besoin de renseignements ?**
**Contactez-nous :**

**01 55 89 08 85**
**clientsfinaux@eset-nod32.fr**

Scannez ce code QR pour télécharger nos documentations ou obtenir gratuitement une version d'évaluation de nos solutions

**www.eset.com/fr**

Plus de 30 ans d'innovation continue

1er éditeur Européen de solutions de sécurité

Focus continu sur la technologie

Croissance continue depuis sa création