Le guide complet de l'XDR :

Menaces actuelles, défis et solutions

Cybersecurity
Progress. Protected.

Comprendre l'XDR

La détection et la réponse étendues (XDR) ne sont plus un concept d'avenir, mais un élément indispensable de l'infrastructure de sécurité d'une organisation. Ce guide est conçu pour aider les professionnels de la sécurité, les responsables informatiques et les décideurs dans leur choix d'une solution de XDR.

Voici ce que vous apprendrez :

- L'évolution du paysage des menaces favorise l'adoption de la technologie de XDR
- Comment la technologie de XDR offre une visibilité, une rapidité et une réponse intégrée
- 9 fonctionnalités essentielles à exiger d'une plateforme moderne
- Implications d'une solution robuste de XDR
- Questions à poser aux fournisseurs
- Comment ESET fournit des solutions de XDR et de MDR dans un écosystème unifié

Qu'il s'agisse de mettre à niveau une infrastructure existante ou d'effectuer votre premier déploiement de XDR, ce document fournit les informations, les listes de contrôle et les stratégies d'évaluation nécessaires pour sécuriser efficacement votre environnement à grande échelle.

Menaces actuelles

Pour comprendre la valeur de l'XDR, il est essentiel de commencer par les menaces qui continuent à peser sur les organisations du monde entier. Plusieurs menaces se sont révélées particulièrement dangereuses au cours des deux dernières années et sont devenues de plus en plus difficiles à combattre sans fonctionnalités avancées de détection intégrée. Ces **menaces** n'exigent pas seulement une meilleure visibilité ; elles **nécessitent une corrélation interdomaine**, **une analyse des comportements** et **une connaissance du contexte en temps réel**. En bref, l'XDR est la réponse.

ATTAQUES DE RANSOMWARES 3.0

Les attaques de ransomwares ont évolué au cours de ces cinq dernières années. De nombreuses opérations modernes utilisent désormais des tactiques de double extorsion, voire triple, combinant le chiffrement, le vol de données et des menaces sur les tiers connectés à la victime afin de maximiser la pression et d'augmenter la probabilité de paiement.

Ces campagnes peuvent être précédées de longues périodes de préparation, souvent de plusieurs mois, au cours desquelles les acteurs de menaces escaladent discrètement les privilèges et exfiltrent des données sensibles.

Le coût moyen d'une atteinte à la sécurité des données était de

4,45 millions USD

Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2025*

En règle générale, cela implique l'exploitation d'identifiants légitimes, le mouvement latéral avec précision, et le contournement des outils cloisonnés, ce qui rend la fusion des données télémétriques entre les différents domaines essentielle à la détection. Les attaquants sont également de plus en plus capables d'exploiter les lacunes dans la réponse, non pas par manque de détections, mais parce qu'elles sont souvent ignorées ou négligées par les défenseurs.

Cette évolution se poursuit avec **la récente découverte par ESET de PromptLock**, le premier ransomware connu **s'appuyant sur l'IA générative**. Il utilise un modèle de langage local pour générer des scripts malveillants de façon autonome, en adaptant son comportement en fonction des requêtes, sans nécessiter de développeurs qualifiés. Ceci marque un tournant : l'IA peut désormais aider les acteurs de menaces à concevoir des attaques dynamiques et multiplateforme. Les malwares générés par l'IA devenant de plus en plus viables, les plateformes de XDR doivent évoluer pour détecter en temps réel les menaces non déterministes en fonction de leur comportement.

TACTIQUES DE SUBSISTANCE ET DE POST-COMPROMISSION

Le détournement d'outils d'administration légitimes est l'un des défis les plus persistants auxquels les défenseurs doivent faire face. Ces outils comprennent PowerShell, PsExec, Windows Management Instrumentation (WMI), et AdFind. Appelés outils LOTL (« living-off-the-land »), ils permettent aux adversaires d'opérer dans les limites de ce qui semble être le comportement normal d'un administrateur.

Ces dernières années, Microsoft a signalé plusieurs cas d'attaques détournant des outils de surveillance et d'administration à distance (RMM) tels que BeyondTrust Remote Support et SimpleHelp, élargissant ainsi les techniques de LOTL pour inclure des plateformes de confiance tierces utilisées par les équipes informatiques elles-mêmes (Microsoft Security). Les attaquants sont en mesure de détourner des outils et des fonctions légitimes au sein d'un système cible pour mener des activités malveillantes.

Certains événements, comme l'arrêt du processus LSASS (Service du sous-système d'autorité de sécurité locale), peuvent déclencher des alertes de haute gravité en raison de leur profil de menace connu. D'autres peuvent sembler inoffensifs s'ils sont isolés, et ne génèrent que des alertes de faible gravité ou des alertes informatives. Cependant, lorsqu'ils sont mis en corrélation avec l'accès aux identités, des mouvements latéraux ou des schémas d'anomalie, leur véritable risque devient évident. C'est **dans ce domaine que les solutions de XDR matures excellent** : **exposer les intentions malveillantes grâce au contexte**. Qu'il s'agisse d'un flot de signaux de faible priorité ou d'une activité subtile, c'est la corrélation qui transforme le bruit en informations exploitables.

EXFILTRATION ET EXPOSITION DES DONNÉES

Il n'est pas surprenant que le vol de données soit souvent l'objectif final, et non un simple effet secondaire. L'exfiltration de données sensibles, par exemple de documents financiers, de propriété intellectuelle, de code source ou d'informations sur les clients, à partir de plateformes de stockage légitimes dans le cloud telles que Dropbox, Google Drive ou OneDrive, continue d'être une tactique très répandue parmi les acteurs de menaces.

Cependant, l'exposition des données n'est pas toujours le fait d'acteurs extérieurs ; des configurations erronées, des erreurs internes ou des contrôles d'accès insuffisants peuvent également conduire à de graves atteintes à la sécurité. Une mauvaise configuration des plateformes SaaS ou du stockage dans le cloud public, la négligence d'un collaborateur ou la compromission d'un compte de service peuvent entraîner des fuites à fort impact. L'XDR identifie ces risques en **détectant les anomalies dans le flux de données et le comportement des utilisateurs**, en particulier lorsque les modèles de trafic sortant s'écartent de la base de référence.

RISQUES LIÉS À L'INTÉGRATION DES IDENTITÉS ET DE LA CHAÎNE D'APPROVISIONNEMENT

La chaîne d'approvisionnement moderne est numérique et profondément interconnectée, englobant des fournisseurs, des plateformes SaaS, des API et des systèmes d'identité fédérée. Les compromissions ne proviennent plus seulement des logiciels ; elles émergent désormais d'autorisations OAuth mal configurées, d'intégrations tierces compromises et de fournisseurs d'identité (IdP), qui sont devenus les nouvelles têtes de pont.

Des incidents récents très médiatisés ont montré comment des attaquants exploitent la mauvaise configuration des systèmes d'authentification unique, des pipelines vulnérables de CI/CD, ou des jetons d'accès pour s'infiltrer dans des environnements par ailleurs sécurisés. Sans **visibilité sur la télémétrie du cloud**, **des endpoints et des identités**, ces voies indirectes de compromission peuvent rester indétectées.

ATTAQUES SUR LES IDENTITÉS ET DÉTOURNEMENTS DE SESSION

Les attaquants savent que les identités sont un périmètre précieux. Des identifiants compromis sont impliqués dans la grande majorité des atteintes à la sécurité, et l'authentification multifacteur (MFA) ne semble plus être un moyen de défense garanti. De nos jours, les adversaires exploitent la lassitude liée à la MFA, le vol de jetons de session et les attaques par réutilisation de cookies pour obtenir et conserver l'accès.

Une fois à l'intérieur, ils opèrent souvent sous des sessions utilisateur valides, ce qui les rend presque invisibles pour certains outils et est une tactique courante de subsistance (LOTL).

80 %

des atteintes à la sécurité

impliquent des techniques basées sur les identités.

Source : *Rapport de Verizon sur les fuites de données en 2025*

L'XDR excelle ici en **suivant la façon dont les identités sont utilisées à travers les systèmes**, **en corrélant le comportement avec les bases de référence connues et en faisant apparaître les anomalies à haut risque**, même lorsque l'utilisateur est authentifié.

ACCÈS EN TANT QUE SERVICE ET COURTIERS D'ACCÈS INITIAL (IAB)

La professionnalisation de la cybercriminalité a donné naissance à l'accès en tant que service (AaaS), où des courtiers d'accès initial (IAB) vendent des points d'entrée dans des réseaux aux gangs de ransomwares et autres acteurs de menaces. Ces points d'accès sont souvent acquis des mois à l'avance et restent inactifs jusqu'à ce qu'ils soient monétisés.

Plus tôt les défenseurs peuvent repérer ces accès initiaux, mieux ce sera pour la sécurité. Ces incidents sont souvent marqués par des événements d'authentification étranges, la réactivation de comptes d'administration dormants ou une reconnaissance à partir de la ligne de commande. L'XDR permet de **repérer des menaces à un stade précoce** et de mener des enquêtes, en catégorisant les événements à faible signal en incidents à forte probabilité.

VOIES D'ATTAQUE PAR LE CLOUD ET LES API

L'infrastructure moderne est dynamique et conçue pour le cloud. Elle repose sur des conteneurs, des microservices, des API et des fonctions sans serveur. Malheureusement, cette agilité s'accompagne d'angles morts. Les adversaires exploitent les vulnérabilités des charges de travail dans le cloud, les API mal configurées, les rôles sur-autorisés et la mauvaise gestion des identités dans le cloud pour se mouvoir dans les réseaux sans toucher les endpoints.

Le périmètre de détection s'est déplacé, et sans visibilité sur la télémétrie du cloud, l'activité du réseau et les journaux des endpoints, les défenseurs ne peuvent avoir une vue d'ensemble. L'XDR comble cette lacune en reliant les signaux des plateformes AWS, Azure, GCP et SaaS à l'activité sur site, pour mettre en évidence les menaces qui se cachent dans les interstices.

Les menaces d'aujourd'hui sont sophistiquées non seulement sur le plan technique, mais également de par leur capacité à **exploiter la fragmentation des outils de sécurité**. Les attaquants comptent sur les angles morts entre les systèmes cloisonnés, qu'il s'agisse des endpoints, du cloud, des identités ou des réseaux.

79 %

des organisations

ont connu au moins un incident de sécurité lié au cloud au cours de l'année écoulée.

Source : *Rapport de la Cloud Security Alliance sur les principales menaces ciblant le cloud en 2024*

Les menaces couvertes ici, depuis les ransomwares furtifs et les détournements d'identités jusqu'aux intrusions dans le cloud et les risques liés aux tiers, soulignent le **besoin urgent d'une détection et d'une réponse interdomaine intégrées**.

L'XDR n'est pas seulement un outil. C'est une réponse à la façon dont les attaquants opèrent aujourd'hui. Les sections suivantes examinent comment la technologie de XDR tient cette promesse, ce qu'il faut rechercher dans une solution, et comment les organisations peuvent la déployer efficacement pour combler les lacunes et reprendre l'avantage.

Comment l'XDR peut vous aider ?

Si la surveillance des événements de bas niveau sur les endpoints peut sembler un bruit de fond pour les équipes de sécurité très occupées, il est temps d'adopter une vision plus étendue. Dans le paysage actuel, où le détournement des identités, la compromission du cloud et les attaques accélérées par l'IA font les gros titres, la **bonne télémétrie** peut faire ou défaire vos défenses. L'XDR ne consiste pas seulement à faire apparaître des alertes, mais également à permettre une visibilité, une prise de décision et une réponse décisive dans l'ensemble de votre parc numérique.

AVANTAGES CLÉS

Les organisations qui déploient l'XDR pour la première fois sont souvent surprises par le nombre et la diversité des événements qui commencent à déclencher des détections. Cette visibilité initiale peut devenir un tournant : elle permet de mettre au jour une mauvaise hygiène liée aux identités, des erreurs de configuration du cloud, l'utilisation non autorisée de SaaS, et des menaces qui avaient discrètement échappé aux contrôles antérieurs. La première vague de déploiement de l'XDR apporte souvent **deux avantages immédiats** : **une meilleure visibilité** sur les lacunes de l'architecture de sécurité et **une identification plus rapide** des menaces précédemment non détectées.

34 %

des dirigeants IT

accordent la priorité à la sécurité du cloud dans leurs investissements de cybersécurité.

Source : *Statista : Priorités d'investissement de cybersécurité pour les leaders du secteur technologique en 2025*

Dans la première section, nous avons exploré les menaces qui sont notoirement difficiles à appréhender sans une détection étendue. Grâce à une approche de XDR moderne, les entreprises peuvent s'attaquer en toute confiance à des problèmes tels que les ransomwares, les malwares destructeurs, les attaques contre la chaîne d'approvisionnement et les menaces internes. Il est tout aussi important de pouvoir détecter l'utilisation détournée d'outils légitimes, tels que les services de stockage dans le cloud utilisés pour l'exfiltration ou les fournisseurs d'identité de confiance utilisés comme point d'entrée.

Les plateformes de XDR actuelles vont au-delà de la corrélation de type SIEM en incorporant des analyses des comportements, un enrichissement du contexte en temps réel, des correspondances MITRE ATT&CK et, de plus en plus, une analyse par l'IA pour mettre en évidence les signes précoces de compromission. Ce sont des fonctionnalités que Forrester a identifiées comme des différentiateurs clés dans son rapport de 2025 sur les plateformes d'analyse de la sécurité.

En se référant aux tactiques et techniques du cadre ATT&CK, les défenseurs peuvent imiter plus précisément les adversaires et **ajuster** leur **couverture** de manière proactive. Au fur et à mesure de l'apparition de nouvelles méthodes (vol de jetons, escalade des rôles dans le cloud et mouvements latéraux entre les IdP), le système de XDR évolue en parallèle.

L'XDR permet également une **recherche moderne des menaces**, afin que les analystes puissent **formuler des hypothèses** et **enquêter sur les endpoints**, **les environnements cloud**, **les identités**, **et les flux réseau**. Grâce à la synthèse et la visualisation par la GenAI, la recherche des menaces peut passer plus rapidement des signaux faibles à des fils d'attaques complets. Cette chasse est devenue non seulement plus efficace, mais également plus accessible à des équipes plus étendues, quel que soit leur niveau d'expérience.

> **« D'ici 2026, plus de 80 % des organisations auront consolidé les équipes et les outils de gestion des endpoints au sein d'une équipe centralisée utilisant une plateforme d'UEM unique, contre environ la moitié début 2022. »**

Gartner : *Consolidation des équipes, des outils et des stratégies de gestion des endpoints pour réduire les coûts et optimiser les opérations, Tom Cipolla, Sean Bankston. [3 juillet 2024] ID : G00778293*

Aujourd'hui, **l'IA intégrée à l'XDR** est passée de la corrélation passive à l'enrichissement actif pour **hiérarchiser les détections à haut risque**, **résumer les chaînes d'attaque**, et même **proposer des étapes de réponse**. Gartner note que les plateformes modernes de XDR s'appuient de plus en plus sur le machine learning pour l'établissement dynamique de bases de référence et sur la GenAI pour la contextualisation des alertes. Cela permet de réduire la charge de travail des analystes et d'accélérer la catégorisation. Dès qu'une menace est découverte, les systèmes de XDR automatisent désormais la réponse, déclenchant des plans d'action qui peuvent isoler un hôte, révoquer un jeton, désactiver un utilisateur ou alerter des intervenants humains.

Cela permet d'accélérer le confinement et de réduire le temps de présence des attaquants, en particulier pendant les heures creuses. Grâce à la corrélation des processus, l'XDR aide les personnes chargées de répondre aux incidents à remonter les alertes jusqu'au point initial de compromission, ce qui permet souvent d'identifier les détournements d'autorisations, les accès de tiers ou les problèmes liés à la chaîne d'approvisionnement des logiciels comme étant les causes profondes.

La technologie de XDR moderne ne fonctionne pas en vase clos. Elle s'intègre étroitement aux plateformes de protection des charges de travail dans le cloud (CWPP), aux outils de sécurité SaaS, aux SIEM et même aux systèmes de CI/CD, offrant ainsi une vision unifiée sur l'infrastructure moderne.

Pour les défenseurs chargés de sécuriser des environnements tentaculaires et hybrides, l'XDR permet de combiner collaboration et partage du contexte.

DÉMONSTRATION DE LA VALEUR DE L'XDR

Il ne s'agit plus de prouver simplement que l'on « dispose de l'XDR », mais de démontrer la valeur mesurable qu'il apporte : au-delà du temps moyen de détection ou de réponse (MTTD/MTTR), la réduction du rayon d'action des atteintes à la sécurité, le triage plus rapide entre les équipes et une vision plus claire des zones où le risque s'accumule, sont tout aussi importants. La possibilité de réduire le coût des outils en fusionnant la détection, l'investigation et l'automatisation en une seule plateforme est devenue un facteur important dans la prise de décisions budgétaires.

52 %

des équipes IT

comptent augmenter leurs investissements dans l'XDR.

Source : *Rapport de la Cloud Security Alliance sur les principales menaces ciblant le cloud en 2024*

Ce qu'il faut rechercher en matière de XDR

COMPRENDRE L'ÉVOLUTION DE L'XDR

Lorsque la technologie de XDR a fait son apparition sur le marché, elle a été saluée comme un moyen d'unifier les signaux d'alerte provenant d'outils de sécurité disparates et de réduire la charge de travail des équipes de SOC. Les premières offres se concentraient sur la corrélation, en regroupant les alertes de l'EDR, de la messagerie et du réseau dans une console unique. Mais aujourd'hui, les attentes ont évolué.

Les plateformes de XDR modernes sont censées non seulement corréler les signaux, mais également **analyser les comportements**, **automatiser la réponse** et **cartographier les attaques** dans des environnements hybrides. Alors que les acteurs de menaces se tournent vers la compromission des identités, le détournement du cloud et l'évasion par l'IA, la portée de l'XDR doit s'étendre pour couvrir les endpoints, les identités, les applications SaaS, les pipelines de CI/CD, et bien plus encore.

Cette évolution signifie que les acheteurs doivent repenser ce qu'est un « bon XDR ». Les critères d'évaluation ont changé : il ne s'agit plus seulement d'agréger des alertes, mais de fournir une aide à l'investigation, une visibilité sur la surface d'attaque et des fonctionnalités de réponse adaptative. Les sections suivantes présentent huit fonctionnalités techniques essentielles et un aspect stratégique que vous devez attendre d'une solution de XDR.

9 ÉLÉMENTS CLÉS À ATTENDRE D'UNE SOLUTION DE XDR MATURE

DÉTECTION

L'XDR doit repérer les menaces qui échappent aux autres outils. Cela signifie faire plus qu'établir une correspondance avec des signatures ou des IoC, et adopter l'analyse des comportements, la télémétrie des identité et les signaux du cloud. **Recherchez des plateformes qui** ne se contentent pas de corréler les événements entre les endpoints, les charges de travail, les utilisateurs et les applications SaaS, mais qui **suivent et reconstruisent des chaînes d'attaque entières** sous la forme d'incidents unifiés.

Ce niveau de corrélation plus approfondi, l'un des principaux atouts d'ESET Inspect, permet aux équipes de sécurité de comprendre comment des événements individuels sont liés entre eux dans le temps et entre les systèmes. C'est précisément cette fonctionnalité qui distingue ESET dans les évaluations MITRE ATT&CK récentes, où ESET Inspect a fait preuve d'une visibilité et d'une contextualisation exceptionnelles à travers les multiples étapes des attaques.

Les meilleures solutions de XDR détectent des techniques telles que le détournement de jetons, le « bourrage d'identifiants », le mouvement latéral via les fournisseurs d'identité (IdP) et les activités liées aux tactiques MITRE ATT&CK connues.

Ces techniques exploitent également la lassitude des victimes potentielles liée à l'utilisation de la MFA ; les attaquants manipulent les utilisateurs pour qu'ils approuvent des demandes d'authentification répétées. La détection devrait également s'intégrer avec la **threat intelligence** et appliquer le machine learning pour supprimer le bruit tout en préservant la fidélité.

À mesure que l'adoption de l'IA s'accélère à la fois dans les outils défensifs et dans les flux de travail des entreprises, les responsables de la sécurité doivent trouver le juste milieu entre innovation et surveillance, d'autant plus que l'utilisation détournée, les fuites de données et l'exposition involontaire deviennent des préoccupations croissantes. Les attaquants commencent également à utiliser l'IA, même si son intégration dans leurs tactiques reste émergente.

Selon le rapport d'IBM sur le coût des atteintes à la sécurité des données en 2025, 97 % des organisations ayant subi des incidents de sécurité liés à l'IA ne disposaient pas de contrôles d'accès adéquat, de nombreuses attaques provenant d'outils tiers ou d'IA non autorisée. Pourtant, ceux qui adoptent l'IA pour la détection et l'automatisation constatent une baisse significative des coûts liés aux atteintes à la sécurité, ce qui confirme que l'**adoption stratégique de l'IA dans l'XDR** améliore l'**efficacité**.

RÉPONSE

La détection n'est que la moitié de l'équation ; c'est dans la réponse que l'XDR apporte une valeur opérationnelle. Recherchez des plateformes qui prennent en charge des **actions de réponse native** sur plusieurs surfaces : isolement des hôtes, désactivation des utilisateurs, révocation des jetons et intégration avec des pare-feu ou des CASB pour contenir les menaces cloud.

61 % des praticiens de sécurité

estiment qu'il existe trop de flux de threat intelligence.

Source : *TechRadar : Une surabondance de sécurité génère plus de données d'alerte que les administrateurs ne peuvent ingérer, ce qui rend la situation encore plus dangereuse.*

Un XDR efficace comprend également l'automatisation pilotée par des guides et s'intègre aux outils de gestion des services informatiques pour une réponse coordonnée. Des politiques de réponse personnalisables et un accès en fonction des rôles sont essentiels pour garantir des actions appropriées sans dépasser les limites.

ÉQUILIBRE

Le bruit reste un point sensible. Une plateforme de XDR mature doit trouver le juste équilibre entre visibilité et exploitabilité. Elle devrait utiliser des scores de gravité, hiérarchiser les risques et créer une base de référence des comportements pour éviter la lassitude liées aux alertes tout en veillant à ce que les menaces réelles ne soient jamais ignorées.

Le **réglage personnalisé**, les **exclusions** et la possibilité de **fournir un contexte autour des alertes**, en indiquant la cause profonde, les ressources touchées et la progression de la chaîne d'attaque, aident les analystes à catégoriser et agir plus rapidement et plus efficacement.

TRANSPARENCE

Les analystes doivent comprendre pourquoi une détection s'est produite et quelle logique a conduit à une alerte. Une **logique de règles transparente**, la **correspondance des détections** avec MITRE ATT&CK, et des chemins de **télémétrie clairement identifiés** sont maintenant attendus de tout grand produit de XDR.

53 %
des alertes cloud

ne sont pas pertinentes, ce qui conduit à des modes de réponse réactifs.

Source : *TechRadar : Une surabondance de sécurité génère plus de données d'alerte que les administrateurs ne peuvent ingérer, ce qui rend la situation encore plus dangereuse.*

La solution idéale serait une plateforme offrant un accès aux données brutes, des explications sur la détection et une évaluation de la gravité. Des points supplémentaires seraient octroyés aux solutions permettant de créer ou de modifier des règles à l'aide de normes ouvertes telles que SIGMA, ou prenant en charge l'intégration dans les pipelines d'analyse via des API.

PERSONNALISATION

Chaque environnement est différent. Il est essentiel de savoir ce qui est normal pour vous. L'adaptation de l'XDR à votre situation est ce qui en fait une puissante solution. Une plateforme de XDR doit permettre aux analystes de définir une logique de détection personnalisée, d'automatiser les réponses en fonction de leurs guides et d'adapter la visibilité aux besoins spécifiques de chaque rôle.

Les **indicateurs personnalisés**, les **règles de détection**, les **requêtes de recherche de menaces** et les widgets de tableau de bord contribuent tous à une meilleure connaissance de la situation afin que les défenseurs de votre organisation puissent atteindre l'équilibre souhaité entre risque et bruit. La prise en charge de l'analyse du comportement des utilisateurs et des entités (UEBA), conçue pour mettre en évidence les comportements anormaux spécifiques à votre base de référence, est indispensable.

INTÉGRATION

La technologie de XDR moderne ne peut pas exister en vase clos. Les meilleures plateformes s'intègrent à un vaste écosystème d'outils tiers : pare-feu, EPP, SIEM, IAM, systèmes de tickets et fournisseurs de threat intelligence. L'intégration devrait être **facile à configurer** et prise en charge par des API robustes.

Alors que certaines solutions se focalisent sur une intégration native, avec de nombreux fournisseurs proposant généralement des systèmes de sécurité sur endpoints et des systèmes de réputation et de détection dans le cloud, de nombreuses équipes de sécurité préfèrent une interopérabilité poussée. Ce qui importe le plus, c'est la **transparence du flux de données**, de l'enrichissement et de la réponse sur l'ensemble de vos investissements existants.

COUVERTURE MULTIPLATEFORME

L'XDR doit couvrir plus que des endpoints. La solution devrait offrir une visibilité sur Windows, macOS, Linux et les appareils mobiles, tout en intégrant les données télémétriques provenant des plateformes cloud (AWS, Azure, GCP), des applications SaaS (M365, Google Workspace, Salesforce) et des systèmes d'identité (Okta, AAD, Ping). Recherchez la prise en charge des charges de travail conteneurisées, des pipelines de CI/CD et de la télémétrie réseau. La possibilité de suivre les **mouvements latéraux** à travers le cloud, les **identités**, et les **endpoints** est indispensable dans le paysage des attaques d'aujourd'hui.

SERVICES

Toutes les organisations ne disposent pas des ressources nécessaires pour doter un SOC d'un personnel complet. Les principaux fournisseurs de solutions de XDR proposent des services managés (MxDR) dans le cadre de leur solution, comprenant surveillance, triage, réponse guidée, recherche des menaces et plus encore.

Même sans externaliser complètement la détection, des services d'assistance à la mise en route, d'aide au réglage et d'optimisation continue peuvent accélérer la rentabilisation. La **maturité du service** pouvant être un facteur de différenciation majeur entre les fournisseurs, il convient donc de veiller à déterminer si le fournisseur offre plus qu'un simple produit :

- 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 en langue locale

FOURNISSEUR

Enfin, évaluez le fournisseur de XDR : présence sur le marché, transparence de la feuille de route du produit, rapidité d'intégration et assistance à la clientèle sont autant d'éléments qui comptent. La validation et les tests par des tiers, tels que les évaluations MITRE ATT&CK® ou les tests Endpoint Prevention & Response (EPR), les évaluations par des pairs et d'autres rapports d'analystes, peuvent aider à distinguer les fournisseurs matures de ceux qui tentent encore de rattraper leur retard.

L'XDR est un investissement stratégique et il est donc dans votre intérêt de vous assurer que la vision du **fournisseur corresponde à votre architecture**, **vos priorités de sécurité**, et **vos contraintes opérationnelles**. Pour ce faire, posez des questions sur la feuille de route, l'engagement en faveur des normes ouvertes, la fréquence des mises à jour et les résultats obtenus dans le cadre d'évaluations indépendantes telles que les évaluations ATT&CK ou Forrester Wave.

Guide de l'acheteur

À mesure que l'XDR devient un pilier central des SecOps modernes, le choix de la bonne plate-forme va bien au-delà de la comparaison des fonctionnalités. Cette liste de contrôle aide les acheteurs à évaluer non seulement les fonctionnalités, mais également l'impact opérationnel, la maturité des fournisseurs et l'adéquation avec l'écosystème.

DÉTECTION ET COUVERTURE

- ☐ Prend en charge l'analyse des comportements et les détections multidomaine corrélées
- ☐ Inclut la télémétrie des identités, des clouds et des SaaS (au-delà des endpoints)
- ☐ Détecte les menaces sophistiquées : vol de jetons, mouvement latéral, lassitude liée à la MFA, etc.
- ☐ S'intègre à la threat intelligence pour une détection enrichie
- ☐ Intègre des correspondances MITRE ATT&CK avec des détails sur la façon dont l'action ou la technique a été réalisée

ENQUÊTE ET RÉPONSE

- ☐ Propose une investigation centralisée avec des scénarios d'attaque ou des chronologies
- ☐ Permet des actions de réponse interdomaine pour coordonner l'isolement des hôtes, la révocation des jetons
- ☐ Inclut des guides automatisés personnalisables
- ☐ S'intègre aux outils d'ITSM pour les tickets d'incident et les flux de travail
- ☐ Réduit le MTTR grâce à une logique de réponse préétablie et des alertes riches en contexte

PERSONNALISATION ET TRANSPARENCE

- ☐ Permet l'édition de règles, des requêtes de recherche de menaces et le réglage de la détection
- ☐ Prend en charge les normes ouvertes (par ex. SIGMA, STIX, OpenTelemetry)
- ☐ Offre une transparence totale sur la logique des alertes et de l'évaluation
- ☐ Fournit un accès aux vues, règles et tableaux de bord en fonction des rôles
- ☐ Permet un feedback transparent pour affiner les performances

INTÉGRATION ET ÉVOLUTIVITÉ

- ☐ Se connecte via des API aux pare-feu, IAM, SIEM et autres outils
- ☐ Prend en charge des infrastructures hybrides/multicloud et des ressources distantes
- ☐ Est suffisamment souple pour s'adapter aux infrastructures technologiques natives des fournisseurs ou aux meilleures technologies
- ☐ Permet une expansion modulaire (par ex. charges de travail dans le cloud, OT, conteneurs)
- ☐ Est prévu pour s'adapter à plusieurs divisions ou sites

SERVICES ET FIABILITÉ DU FOURNISSEUR

- ☐ Offre des services de mise en route, de réglage et d'optimisation continue
- ☐ Comprend l'accès à une assistance technique locale et présence de partenaires
- ☐ Fournit un accès à la recherche de menaces ou au MxDR (au besoin)
- ☐ A une feuille de route claire et des mises à jour régulières des produits
- ☐ Est validé par des tests tiers (évaluations ATT&CK, Forrester Wave, évaluations par des pairs)

LES INCONTOURNABLES

- ☐ Détection corrélée sur les endpoints, le cloud et les identités
- ☐ Guides de réponse automatisés et personnalisables
- ☐ Intégration via des API ouvertes
- ☐ Logique de détection transparente
- ☐ Correspondance précise avec les techniques MITRE ATT&CK
- ☐ Prise en charge linguistique ou partenaires de service régionaux

LES SOUHAITABLES

- ☐ Assistants de recherche de menaces par la GenAI
- ☐ Modules intégrés de reporting exécutif
- ☐ Attribution à des acteurs de menaces
- ☐ Prise en charge native de la télémétrie OT/IoT

COMMENT ÉVITER LES PROMESSES EXCESSIVES DES FOURNISSEURS

Dans un secteur aussi dense et en pleine évolution que celui de l'XDR, il est facile de se laisser convaincre par de belles démonstrations et des affirmations audacieuses. Insistez sur les preuves : évaluations par des tiers (comme les évaluations ATT&CK®), études de cas clients et calendriers de déploiement réalistes.

Demandez si une fonctionnalité est généralement disponible, en accès anticipé ou simplement sur la feuille de route. **La clarté dès le départ évite les déceptions après l'achat**.

QUESTIONS CLÉS POUR UN APPEL À PROPOSITIONS

- Quelles sont les sources de données intégrées de manière native et quelles sont celles qui nécessitent des connecteurs personnalisés ?
- Comment votre plateforme prend-elle en charge la détection des menaces basées sur les identités ?
- Quels types d'actions de réponse sont automatisés et prêts à l'emploi ?
- Comment les règles de détection sont-elles adaptées et mises à jour au fil du temps ?
- Pouvez-vous présenter des correspondances MITRE ATT&CK et des résultats d'évaluations récentes ?
- Quels sont les services inclus dans la mise en route et l'optimisation ?
- Un support est-il disponible dans notre région et notre langue ?

Le marché de l'XDR continuera d'évoluer, mais les principes de visibilité, d'intégration et d'efficacité opérationnelle resteront au cœur de tout programme robuste de sécurité.

Utilisez la liste de contrôle ci-dessus non seulement pour comparer les fournisseurs, mais également pour **définir la valeur que vous attendez** de votre plateforme de détection et de réponse de nouvelle génération.

Renforcez votre XDR avec ESET

L'utilisation de l'analyse des comportements 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 de 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 de XDR** dans le cloud capable de :

- Détecter les menaces persistantes avancées
- Stopper les menaces en mémoire
- Bloquer les menaces zero-day
- Protéger contre les ransomwares
- Empêcher les atteintes à la politique de sécurité de l'entreprise

LES AVANTAGES ESET

Prévention, détection des réponse totales

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 de l'IA, du Cloud, et maintenant de l'XDR.

Mieux vaut prévenir que guérir

L'approche d'ESET en matière de XDR est étroitement liée à ses produits de prévention primés. Grâce à son engagement à développer une technologie de détection de haute qualité, la technologie de prévention d'ESET est une des meilleures du secteur.

Visibilité détaillée sur le réseau

Avec des règles de détection transparentes (ESET en compte plus de 1620), des indicateurs de compromis (IoC) 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®, 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 de ne pas inclure les applications légitimes 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 personnalisation

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 DE 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 de 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 d'une **threat intelligence globale** issue d'ESET LiveGrid®.

ESET Inspect surveille les événements d'authentification, les escalades de rôles dans le cloud et les schémas d'accès SaaS pour détecter les mouvements latéraux, les détournements de jetons et de l'authentification OAuth. Combinée à la corrélation d'identités et la détection d'anomalies, cette fonctionnalité permet à la plateforme ESET PROTECT de **lutter contre les menaces basées sur les identités les plus insaisissables à l'heure actuelle**.

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.

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.

Qualité

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

Transparence

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

DE L'XDR AU MDR : SÉCURISÉ ET RATIONALISÉ

ESET XDR offre une détection transparente, basée sur le comportement, une recherche avancée des menaces et une investigation rapide des incidents sur différentes couches : endpoints, messagerie, SaaS et identités. Pour les organisations qui souhaitent se concentrer sur leurs opérations principales, ESET propose **ESET PROTECT MDR**, un service managé 24/7 qui **associe ce puissant moteur de XDR à une surveillance dirigée par des experts**, la recherche de menaces, la réponse aux incidents et l'assistance à la remédiation.

La transition entre le XDR autogéré et le MDR d'ESET est simple : la même technologie, ESET Inspect, est intégrée à votre environnement, puis l'équipe mondiale d'ESET prend en charge la gestion de la détection, le triage des alertes et les tâches de réponse automatisée. Les clients bénéficient d'un **MTTR, parmi les plus courts du marché, de 6 minutes**, d'une recherche proactive des menaces et d'une threat intelligence provenant de plus de 100 millions d'endpoints à travers le monde, le tout sans avoir à recruter de personnel interne spécialisé dans la cybersécurité.

Avec ESET MDR, les équipes gardent le contrôle via la console ESET PROTECT, mais bénéficient en plus d'un service continu, d'un réglage optimisé de la détection, d'une prise en charge des langues locales et de rapports conformes. Le résultat ? Une posture de sécurité renforcée fournie sous la forme d'un service entièrement managé.

Ce modèle de MDR est particulièrement efficace contre les techniques furtives telles que les détournements d'identité et les attaques LOTL, par lesquelles les adversaires opèrent sous des identifiants valides ou utilisent des outils intégrés tels que PowerShell et WMI pour échapper à toute détection.

Les experts d'ESET analysent les écarts par rapport à la base de référence de l'utilisateur et du système afin de détecter ces menaces à un stade précoce, avant qu'un mouvement latéral ou une escalade de privilèges ne se produise.

Au sein du MDR, la visibilité est assurée par la **télémétrie des endpoints et de la messagerie** provenant des solutions de sécurité ESET, ce qui permet une détection fiable de l'utilisation détournée d'outils légitimes et des techniques furtives des pirates. Pour les organisations qui adoptent l'offre plus étendue de cybersécurité managée d'ESET, cette couverture **peut être élargie à d'autres périmètres**, y compris les identités, le réseau et les services cloud, pour éliminer les angles morts et permettre des actions de réponse de haute confiance sans submerger les équipes internes avec du bruit et des faux positifs.

22 %
des dirigeants IT

accordent la priorité aux services managés pour leurs investissements de cybersécurité.

Source : *Statista : Priorités d'investissement de cybersécurité pour les leaders du secteur technologique en 2025*

Conclusion

La promesse de l'XDR ne réside pas dans des acronymes prétentieux, mais dans des résultats tangibles : réduction du temps de présence des attaquants, meilleure visibilité, et prise de décisions plus intelligente et plus rapide. Alors que les acteurs de menaces exploitent les identités, les mauvaises configurations du cloud et les intégrations SaaS, la capacité de corrélation multidomaine et d'automatisation de la réponse n'est plus optionnelle.

Ce guide explore à la fois l'évolution du paysage des menaces et ce que les acheteurs modernes devraient exiger d'une plateforme de XDR :**visibilité**, **intégration**, **transparence**, et **prise en charge**. Les offres de XDR et de MDR d'ESET répondent directement à ces besoins et permettent aux équipes de sécurité d'augmenter leurs capacités sans augmenter leurs effectifs. Qu'il s'agisse d'une gestion autonome ou d'une externalisation complète, la voie à suivre est claire : rendre la détection et la réponse extensibles, adaptables et centrées sur ce qui compte le plus — la cyber-résilience.

EN SAVOIR PLUS SUR L'XDR

ÉTUDE DE CAS D'UN CLIENT DE L'XDR

Kohlpharma

Basé en Allemagne, Kohlpharma est l'un des principaux importateurs européens de produits pharmaceutiques. Depuis 1979, l'entreprise contribue à réduire le coût des soins en fournissant des médicaments de marque à des prix abordables, en s'appuyant sur une logistique avancée et en mettant l'accent sur la cybersécurité. L'entreprise emploie 800 personnes et garantit un accès rapide aux médicaments dans toute l'Allemagne.

En tant que fournisseur d'infrastructures critiques, Kohlpharma avait besoin d'une solution de sécurité pour protéger ses systèmes logistiques automatisés contre les cybermenaces, ce qui nécessitait à la fois des outils antimalwares et des outils avancés de détection et de réponse sur les endpoints (EDR). L'entreprise était de plus en plus ciblée et les enjeux étaient élevés : toute perturbation pouvait entraîner des pertes de plusieurs millions de dollars et éroder la confiance des patients et des partenaires.

ESET a fourni une configuration de sécurité multicouche comprenant ESET PROTECT Entry, LiveGuard Advanced et Inspect. Le déploiement sur 1 250 endpoints a été réalisé en six semaines seulement, avec une collaboration transparente et une mise en œuvre rapide. Les taux de détection élevés d'ESET, sa communication transparente et son rapport coût-bénéfice en ont fait un choix évident.

AVANTAGES CLÉS

- Protection avancée et robuste des infrastructures critiques et des systèmes automatisés
- Déploiement rapide sur 1 250 endpoints en six semaines
- Détection des menaces cloud pour les malwares inconnus et évasifs
- Administration centralisée grâce à des consoles intuitives et faciles à utiliser

> « Une solution de cybersécurité complexe doit fonctionner correctement tout en étant facile à utiliser. ESET maîtrise cet équilibre de manière exemplaire. »

Stefan Pistorius
RESPONSABLE EDP ET ADMINISTRATION, KOHLPHARMA

À propos d'ESET

Défense proactive. Minimisez les risques par la prévention.

Conservez une longueur d'avance sur les cybermenaces connues et émergentes **grâce à notre approche axée sur l'IA et la prévention.** Nous combinons la puissance de l'IA et l'expertise humaine pour améliorer l'efficacité et la facilité d'utilisation de la protection.

Bénéficiez d'une protection **de haut niveau** grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus.

ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie. Progress. Protected.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset®
Cybersecurity
Progress. Protected.