kaspersky BRING ON THE FUTURE

EDR : guide de l'acheteur

Investissez dans la protection EDR optimale pour votre entreprise

En résumé

Pendant des années, les PME ont pu compter sur leur plateforme de protection des terminaux (EPP) pour se défendre contre un large éventail de menaces basiques. Mais avec la transition progressive des cybercriminels vers les menaces nouvelles, inconnues et évasives capables de contourner l'EPP, l'heure est venue de mettre à niveau ces défenses au moyen de solutions de détection et de réponse au niveau des terminaux (EDR) et/ou de détection et réponse gérées (MDR) qui puissent protéger contre de telles menaces.

Ce guide d'achat vous explique comment identifier la sécurité de type EDR qui convient le mieux à votre entreprise en huit étapes simples. Vous devrez d'abord examiner votre protection des terminaux existante pour identifier toute éventuelle faille critique au niveau des défenses de vos terminaux. Vous devrez également déterminer votre objectif avec précision, et identifier la protection la plus adaptée à vos besoins en pensant à vos cas d'utilisation. Intéressez-vous sérieusement aux solutions EDR et MDR, réfléchissez-y en tenant compte de votre environnement de sécurité étendu et dressez une liste des fonctionnalités clés requises chez les éditeurs potentiels.

La lecture de ce guide vous permettra de comprendre les raisons pour lesquelles il est important de mettre vos défenses à niveau et la façon d'y parvenir. Il vous montrera également les avantages offerts par les solutions disponibles et la méthode de création d'une solution de sécurité optimale qui répond aux besoins de votre entreprise et qui soit compatible avec les compétences spécifiques en matière de sécurité de votre équipe informatique.

Pourquoi mettre à niveau vos défenses, et pourquoi le faire maintenant ?

Les solutions de cybersécurité avancées comme la détection et la réponse au niveau des terminaux (EDR) font partie des sujets les plus épineux sur le marché, à juste titre, notamment si votre entreprise est une PME.

Pourquoi cibler ces segments en particulier ? Les changements du paysage de la cybersécurité impliquent que les attaquants d'aujourd'hui ciblent les organisations de toutes tailles, tous types d'activités et tous niveaux de préparation. Plus précisément, les grosses PME se trouvent dans la ligne de mire des menaces

évasives les plus sophistiquées qui ne ciblaient auparavant que les organisations bien plus importantes.

En réaction, les équipes de sécurité informatique complètent leurs plateformes de protection des terminaux existantes (EPP) avec des solutions EDR et/ou de détection et de réponse gérées (MDR) qui leur permettent de détecter et d'étudier les incidents de sécurité, de contenir la menace au niveau du terminal et d'y remédier au moyen d'une réponse et/ou recommandation automatisée.

Malheureusement, l'adoption de ces solutions peut parfois provoquer autant de problèmes qu'elle en résout en alertant les équipes de sécurité d'un énorme volume de menaces qui, bien que suspectes et nécessitant une enquête, s'avèrent finalement inoffensives. Cette situation peut se révéler particulièrement problématique pour les équipes informatiques à faible expertise en matière de sécurité en interne ou ayant trop peu de temps pour gérer ces alertes.

Optimisez vos ressources clés et concentrez-vous sur votre cybersécurité, plutôt que de chasser les faux positifs et les énormes volumes d'alertes.

La solution idéale consiste de ce fait à compléter la protection des terminaux par une sécurité de type EDR : plus on prévient de menaces, moins on reçoit d'alertes que les équipes de sécurité auront à examiner. Les équipes de sécurité informatique peuvent alors optimiser les ressources clés et se consacrer pleinement à la cybersécurité, au lieu de chasser les faux positifs et les énormes volumes d'alertes.

Quels changements du panorama des menaces entraînent donc un besoin de protection plus avancée ? Dans quelle mesure varient-ils pour différents types d'entreprises ? Et (probablement le plus important de tout, compte tenu de la pénurie mondiale de talents qualifiés dans le domaine de la cybersécurité) comment pouvez-vous contrer ces menaces avec une solution qui convient le mieux à votre organisation, à la taille et aux compétences en matière de sécurité de votre équipe informatique, et aux types de cyberattaques auxquelles vous êtes potentiellement exposé ?

Ce guide d'achat vous permettra de répondre aux interrogations suivantes :

- Pourquoi la protection présente actuellement sur vos terminaux n'est-elle pas suffisante contre les toutes dernières menaces ?
- Comment évaluer vos nouveaux besoins en matière de sécurité ?
- Comment identifier la protection la plus adaptée à vos besoins, que ce soit en termes de menaces qui pèsent de plus en plus sur vous et de compétences en matière de sécurité de votre équipe informatique ?
- Que faut-il faire si vous disposez de peu de temps, de peu d'effectifs et d'une expérience réduite en interne en matière de sécurité ?
- Comment les solutions les plus récentes s'adaptent-elles aux environnements de sécurité étendus ?

Pourquoi la sécurité des terminaux existante ne vous protègera pas contre le nouveau panorama des menaces

Pour améliorer la sécurité de vos terminaux, il serait simple de penser qu'il suffit juste d'identifier et de mettre en œuvre une solution EDR qui semble bien convenir à votre entreprise. De la même manière qu'il n'est pas recommandé d'ajouter un étage supplémentaire à un immeuble avant d'en avoir vérifié les fondations, vous devez d'abord examiner votre solution EPP existante.

IDC[1] a formulé la proposition suivante :

- Avant de discuter des éléments à prendre en compte pour votre EDR, IDC recommande en premier lieu d'examiner votre solution EPP existante. Celle-ci doit avoir pour mission de protéger les terminaux en tant que solution indépendante.
- N'acceptez pas de solution EPP médiocre ou peu performante, car elle corrompt les résultats de la solution complète. Une entreprise ne doit pas compenser une solution EPP peu performante par un outil EDR (et beaucoup de temps accordé par un analyste de la sécurité).

N'acceptez pas de solution EPP médiocre ou peu performante, car elle corrompt les résultats de la solution complète pour terminaux[1]. Une entreprise ne doit pas compenser une solution EPP peu performante par un outil EDR (et beaucoup de temps accordé par un analyste de la sécurité).

L'EPP joue un rôle vital en permettant à une entreprise de se protéger contre un large éventail de menaces basiques et de minimiser les charges de travail alouées à la sécurité informatique. Mais dans le cas de menaces évasives, il faut passer à la vitesse supérieure.

Pour réduire les risques présentés par le nouveau panorama des menaces, vous devez commencer par évaluer l'efficacité de la protection de vos terminaux et identifier toute faille potentielle au sein de vos défenses.

Pourquoi votre protection n'est peut-être pas aussi solide que vous le pensez ?

Même si vous estimez avoir une entreprise bien protégée, on estime à près de **4 000** le nombre de violations de données[2] survenues rien qu'au premier semestre 2019, lesquelles ont mis en danger les données de plus de quatre milliards d'utilisateurs.

Ce chiffre alarmant figure dans l'introduction du rapport économique sur la sécurité informatique en 2019 de Kaspersky, qui résume les résultats de notre enquête annuelle mondiale sur les risques liés à la sécurité informatique pour les entreprises. Cette enquête comprend des entretiens avec près de 5 000 PME et grandes entreprises dans 23 pays et a dévoilé quelques-unes de ces statistiques inquiétantes. Par exemple :

55 %

des organisations sont « totalement convaincues » que leur réseau n'a pas été piraté, même si 38 % ont l'impression de manquer de connaissances sur les menaces qui pèsent sur leur activité.

12 %

seulement des grandes entreprises s'inquiètent au sujet des infections par un programme malveillant, bien qu'il s'agisse de l'incident de sécurité le plus coûteux pour elles.

51 %

des grandes entreprises et 47 % des PME conviennent qu'il devient de plus en plus difficile de faire la différence entre les attaques de sécurité génériques et ciblées.

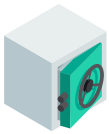
66 %

des grandes entreprises et des PME ont cherché à embaucher davantage de personnel spécialisé en informatique en 2020, en dépit des graves pénuries mondiales, notamment en cybersécurité.

1 IDC Doc n° US45794219, Sécurité des terminaux 2020 : La résurgence de la protection des terminaux et la destinée manifeste de l'EDR - Jan 2020

2 https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Ces chiffres sous-tendent un dangereux décalage entre les perceptions qu'ont les organisations du panorama des menaces, les types d'attaques qui présentent les plus grands risques (y compris financiers) et leur préparation et capacité à se défendre.



L'infection des appareils d'une entreprise par un programme malveillant constitue la forme de violation de données aux répercussions financières les plus lourdes (**2,73 M USD** en 2019), alors que seules 12 % des entreprises sont « très inquiètes » de la menace que représente une telle attaque.

Les PME ignorent également les formes d'attaques qui leur coûtent le plus cher. Les incidents affectant l'infrastructure informatique hébergée par un tiers représentent le type de violation de données le plus coûteux pour les petites entreprises (jusqu'à **162 000 USD**). Les PME ne le classent toutefois qu'à la cinquième place des mesures les plus importantes et se préoccupent avant tout des problèmes liés à la protection des données comme la perte physique d'un appareil ou la perte de données suite à une attaque ciblée.

Les difficultés accrues des grandes entreprises et des PME à distinguer les attaques de sécurité génériques et ciblées leur complique la tâche en termes de détection ou d'évaluation des dangers que représentent les incidents dont elles sont victimes. Ceci explique peut-être les niveaux croissants de menaces de programmes malveillants modérés et avancés auxquels elles s'exposent.

Le rapport a conclu en déclarant qu'« il est vital pour les entreprises de continuer d'investir et de repenser leurs processus de sécurité informatique afin de garder un temps d'avance sur la croissance des cybermenaces, et de limiter les potentielles pertes financières. » Elles ne peuvent toutefois y parvenir qu'en gérant efficacement les menaces réelles auxquelles elles sont de plus en plus exposées, par exemple en investissant dans la sécurité de type EDR nécessaire pour se protéger contre les menaces évasives.

Étape 1 : Examinez la protection présente sur vos terminaux

Avec autant de solutions de cybersécurité avancées disponibles sur le marché, on oublie facilement le rôle vital que joue la protection des terminaux. En quoi les terminaux sont-ils si importants ? En plus de constituer les points d'entrée les plus communs dans l'infrastructure d'une entreprise, ainsi que la principale cible des cybercriminels, ils représentent les sources clés des données nécessaires pour examiner efficacement les incidents complexes.

Par conséquent, chaque organisation doit choisir une solution EPP qui assure une protection automatisée contre un grand nombre d'incidents possibles causés par des menaces basiques, notamment les menaces sans fichiers et les ransomwares.

En raison du niveau relativement limité de connaissances ou d'employés spécialisés en sécurité qu'il exige, ce type de configuration répond aux besoins de sécurité des terminaux des PME ou des petites entreprises ne disposant pas d'une équipe de sécurité dédiée, ou des organisations dotées de faibles niveaux d'expertise en cybersécurité.

Il s'agit de même d'une étape fondatrice essentielle pour les entreprises moyennes et plus grandes où, en traitant automatiquement un grand nombre de menaces mineures, la solution ouvre la voie aux équipes de sécurité qui peuvent alors se concentrer sur une défense plus sophistiquée si nécessaire.

En examinant votre solution EPP pour vérifier qu'elle offre les fonctionnalités attendues, vous devez prendre en compte les aspects suivants :

À quel point cette solution est-elle efficace ?

Combien de faux positifs recevez-vous ?

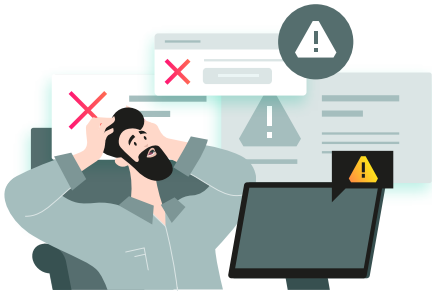
Cette solution offre-t-elle des fonctionnalités de réduction de la surface d'attaque efficace comme le contrôle du Web, des applications et des appareils ?

Permet-elle d'automatiser les tâches routinières ?

Est-elle simple à faire fonctionner et aide-t-elle à minimiser les coûts et les frais administratifs liés à votre équipe informatique ?

Améliore-t-elle l'exécution des tâches essentielles comme l'évaluation des vulnérabilités et la gestion des correctifs ?

Étape 2 : Identifiez toute éventuelle faille critique au niveau des défenses de vos terminaux.



Même si votre EPP vous protège contre un large éventail de menaces basiques, vous devez aussi réfléchir à votre défense contre les menaces nouvelles, inconnues et évasives qui contournent votre EPP.

La préparation d'une attaque revient de moins en moins cher, ce qui expose de plus en plus d'organisations aux risques. En plus de survenir plus fréquemment, ces types d'attaques ont énormément gagné en efficacité en raison des diverses techniques que les criminels combinent, testent et utilisent pour contourner efficacement la sécurité des terminaux.

Le besoin urgent de gérer ces menaces est devenu de plus en plus vital de par les changements tels que la dissolution du périmètre des entreprises découlant de la hausse du travail à distance.

Voici les signes avant-coureurs indiquant qu'il est temps d'étendre vos défenses au-delà de la solution EPP traditionnelle :

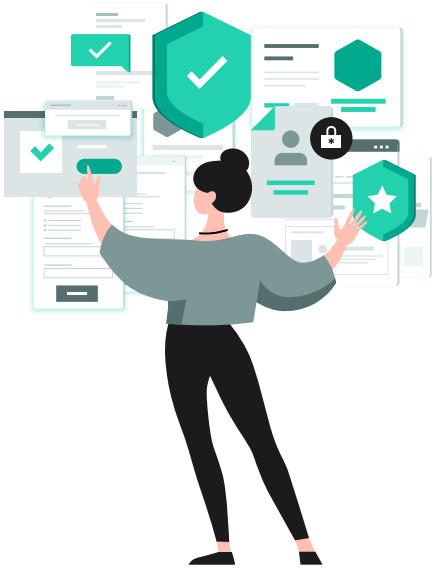
- Votre EPP ne parvient pas à bloquer un nombre croissant de menaces nouvelles, inconnues et évasives.
- Vous disposez d'une visibilité limitée sur ce qui se passe au niveau de vos terminaux. Cela inclut l'incapacité de réaliser une analyse des causes profondes, une enquête et une réponse en temps réel aux menaces, ou l'obligation de devoir le faire manuellement au moyen d'outils de systèmes d'exploitation (OS) standard au cas par cas. Un processus long, complexe et source d'erreurs.
- Vous ne disposez pas des compétences ou capacités spécialisées en sécurité informatique nécessaires pour gérer des menaces toujours plus sophistiquées.
- Les amendes potentielles ou les atteintes à la réputation de votre entreprise résultant d'un incident de sécurité majeur vous inquiètent.

Il sera préférable d'utiliser de façon optimale toutes les fonctions dont vous avez vraiment besoin, plutôt que de payer pour un grand nombre de fonctionnalités qui ne vous serviront pas spécialement

Pour mettre en œuvre une solution efficace capable de vous défendre contre ces menaces, vous devrez prendre en compte les aspects de votre organisation comme sa taille, son profil entreprise, son degré de préparation à la sécurité, ses ressources et son expertise existantes et plus particulièrement le niveau de compétences (ou « maturité ») en matière de sécurité de votre infrastructure informatique ou équipe de sécurité informatique.

Vous aurez également besoin d'une solution qui utilise de façon optimale toutes les fonctions qui vous sont vraiment nécessaires, au lieu de payer pour un grand nombre de fonctions dont vous ne voulez pas vraiment et de devoir recruter des experts en sécurité informatique possédant les compétences requises pour s'en servir.

Étape 3 : Identifiez avec précision l'objectif à atteindre



D'après Gartner[3], les outils EDR offrent une méthode grâce à laquelle les techniciens de la sécurité et de la gestion des risques peuvent répondre à deux questions clés au sujet de la sécurité de leur environnement :

- Que s'est-il passé ?
- Que se passe-t-il maintenant ?

Bon nombre d'organisations disposent d'une expertise limitée (ou d'un petit service de sécurité informatique sans aucun projet d'agrandissement), mais doivent comprendre ce qui se passe dans leur infrastructure et être capables de répondre aux menaces évasives avant qu'elles ne puissent leur nuire.

L'ajout de fonctionnalités EDR appropriées à une solution EPP peut fournir une défense très efficace contre les menaces plus sophistiquées et évasives. Les spécialistes de la sécurité informatique devraient alors obtenir les informations et les connaissances nécessaires à une enquête efficace et les outils requis pour une analyse des causes profondes afin de créer des indicateurs de compromission (IoC) personnalisés, d'importer des IoC et de les analyser à travers tous les terminaux. Et on devrait ainsi pouvoir envoyer des réponses « en un seul clic » automatisées et/ou rapides et précises (mise en quarantaine de fichiers, isolation de l'hôte, interruption d'un processus, suppression d'un objet, etc.).

Étape 4 : Identifiez la protection la plus adaptée à vos besoins

De nombreuses entreprises n'ont pas d'expert de la sécurité dédié. Certaines d'entre elles commencent peut-être tout juste à créer leur service de sécurité informatique, tandis que d'autres disposent sans doute déjà d'équipes de sécurité informatique pleinement formées et compétentes. La qualité de l'expertise disponible de ces organisations en matière de défenses contre les menaces varie donc énormément, à l'instar du temps qu'elles peuvent consacrer à cette tâche.

Pour gérer ces circonstances différentes, les organisations dépourvues de personnel de sécurité informatique dédié ou dont celui-ci est surchargé par les tâches routinières devront utiliser l'automatisation de façon stratégique pour contrer les nouvelles menaces évasives.

Ceci implique de combiner leur EPP avec des outils EDR supplémentaires qui, en plus de protéger contre ces menaces, intègrent des niveaux appropriés d'automatisation (complète ou partielle).

3 Gartner – Comparaison de solutions pour les technologies de détection et de réponse au niveau des terminaux – Jan 2020

Des outils aussi simples d'utilisation que possible, pour gagner du temps et réduire la frustration

Alternative possible : au lieu d'investir dans une solution EDR excessivement complexe pour laquelle elles n'ont pas forcément ni le temps ni les compétences nécessaires, la solution de détection et de réponse gérées (MDR) leur donne un accès à des fonctionnalités comme la surveillance sécurisée 24 h/24, 7 j/7 par des experts, la recherche de menaces automatisée et gérée et les scénarios de réponse à distance guidés, que ce soit auprès d'un fournisseur, d'un fournisseur de services gérés (MSP) ou d'un fournisseur de services de sécurité gérés (MSSP).

En troisième option, il est possible de combiner l'EDR avec une solution MDR. Puisque de nombreuses organisations ne disposent pas de l'expertise requise pour la recherche de menaces, l'idéal consiste souvent à externaliser cette tâche tout en mettant en œuvre les fonctionnalités de détection et de réponse en interne. Ceci peut s'avérer particulièrement bénéfique pour les entreprises qui souhaitent élaborer leur propre équipe de cybersécurité, mais ne possèdent pas les ressources, la main-d'œuvre et/ou les compétences nécessaires pour prendre en charge la détection et la réponse spécialisées.

Quelle que soit la solution la plus adaptée à votre situation, vous aurez besoin d'outils aussi simples d'utilisation que possible, pour gagner du temps et réduire la frustration. Pour minimiser la fatigue à l'égard des alertes, vous devrez également disposer d'une solution qui gère automatiquement un grand nombre de menaces potentielles.

Étape 5 : Pensez à vos cas d'utilisation

Pour identifier la protection qui convient le mieux à vos besoins, vous devez définir des exigences précises à cet égard. Ceci implique de prendre en compte les aspects critiques des performances et de l'utilisation régulière de la solution, comme les cas d'utilisation qu'elle doit exécuter et les résultats qu'elle est censée donner.

À titre d'exemple, quand vous recevez une alerte de sécurité, la solution EDR et/ou MDR doit vous permettre de répondre à des questions clés telles que :

Dans quel contexte l'alerte a-t-elle été lancée ?

Quelles mesures ont déjà été prises à la suite de l'alerte ?

La menace détectée est-elle toujours active ?

D'autres hôtes font-ils l'objet d'une attaque ?

Quel chemin l'attaque a-t-elle emprunté ?

Quelles sont les causes profondes de la menace ?

Elle doit aussi vous aider à visualiser l'ampleur de la menace. Par exemple :

Si une menace globale pèse sur votre entreprise, vos dirigeants voudront sûrement s'assurer que vous n'êtes pas actuellement la cible d'une attaque, auquel cas vous devrez être capable de trouver un IoC en ligne, d'exécuter une analyse et de répondre correctement à leurs préoccupations.

Si les autorités réglementaires vous demandent d'exécuter l'analyse d'un IoC spécifique, vous devez pouvoir importer des IoC issus de sources fiables et exécuter des analyses régulières pour identifier tout signe d'attaque.

Si vous avez examiné en détail une alerte et créé un IoC sur la base des menaces identifiées, vous devez faire automatiser l'exécution des analyses sur l'ensemble du réseau afin de découvrir si d'autres hôtes ont été impactés au lieu de vous en charger vous-même.

De même, vous devez être capable de répondre rapidement à des menaces prolifiques en constante évolution :

- En contenant la menace par l'isolation de l'hôte, la mise en quarantaine du fichier ou la prévention de l'exécution des fichiers pendant l'enquête.
- Par une réponse automatisée sur plusieurs terminaux sur la base d'analyses d'IoC, qui permet de répondre aux menaces évasives instantanément.
- Et, très important, par des scénarios de réponse à distance guidés si vous utilisez une solution MDR.

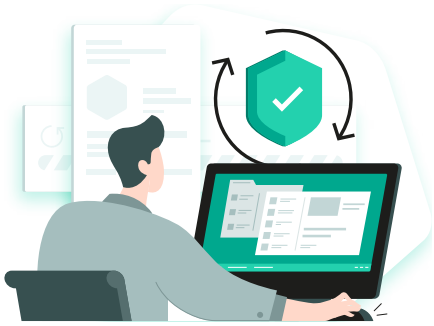
Les résultats clés que vous devez attendre de votre solution incluent les éléments suivants :

- Protection contre les menaces évasives plus fréquentes et plus perturbatrices.
- Économie de temps et de ressources grâce à un outil automatisé et simplifié.
- Visualisation de l'ampleur des menaces complexes sur l'intégralité du réseau.
- Compréhension des causes profondes de chaque menace et de son origine.
- Éviction des dommages préjudiciables par le biais d'une réponse rapide et automatisée.

Et si vous ne disposiez que d'une expertise de sécurité limitée en interne ?

Supposons que vous possédiez une expertise de sécurité limitée en interne, ou une petite équipe composée d'un ou deux spécialistes de la sécurité. Supposons également que vous deviez déterminer la nécessité de compléter votre EPP par une solution EDR et/ou MDR. Quels types d'avantages pouvez-vous attendre et quelle solution vous conviendrait ?

Étape 6 : Intéressez-vous sérieusement aux solutions EDR et MDR



Si vous préférez une approche plus pratique (et que votre équipe informatique possède des compétences suffisamment matures en matière de sécurité informatique), l'EDR peut empêcher les interruptions d'activité et les dommages en éliminant les risques inhérents aux menaces nouvelles, inconnues et évasives et en donnant à votre personnel de sécurité la visibilité nécessaire pour enquêter sur les menaces, analyser leurs causes profondes et y répondre.

Cette solution favorise les économies en permettant à votre équipe de sécurité de travailler plus efficacement sans avoir à jongler avec plusieurs outils et consoles et optimise la capacité en automatisant un grand nombre de processus. Vous aurez également l'esprit tranquille, car il vous sera alors plus facile de surveiller et de détecter les menaces, ainsi que de répondre aux attaques et de les prévenir.

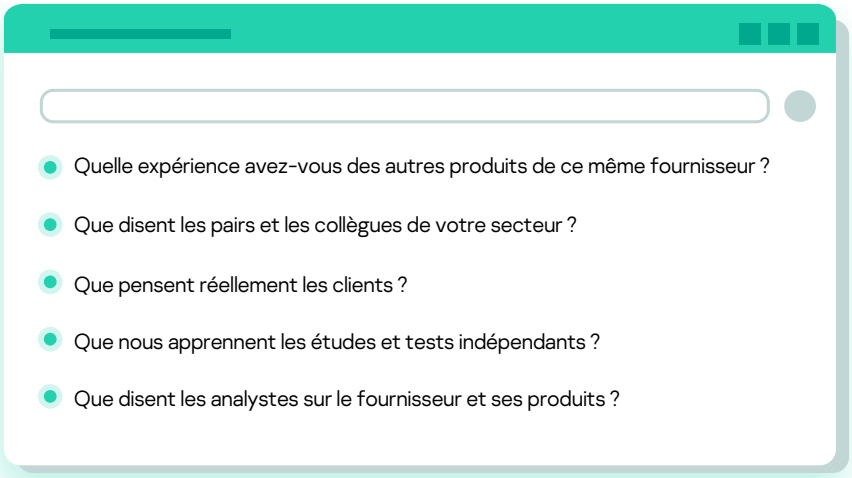
Si vous cherchez à étendre vos capacités de sécurité informatique en interne en déléguant les tâches principales de détection et de réponse, le MDR peut vous offrir une protection avancée et continue contre les menaces qui peuvent contourner les barrières de sécurité automatisées. Cette solution contribue à développer votre entreprise en résolvant la problématique de recrutement de talents dans le domaine de la cybersécurité et en apportant tous les avantages principaux d'un centre d'opérations de sécurité (SOC) 24 h/24, 7 j/7, sans les frais exorbitants y afférents.

La technologie MDR peut également vous permettre de réaliser des économies en réservant les ressources internes aux tâches critiques qui requièrent vraiment l'implication de votre équipe de sécurité informatique, et optimiser la capacité en exploitant des modèles de Machine Learning avancé pour augmenter de manière significative le rendement des analystes et minimiser le délai d'intervention moyen. Cette solution vous assure une surveillance sécurisée continue par des experts, ainsi qu'une recherche de menaces automatisée et gérée. Ceci inclut l'analyse de menaces non malveillantes complexes et les menaces dangereuses difficiles à détecter à l'aide d'outils OS légitimes dans les attaques.

En parallèle, la combinaison de solutions EDR et MDR vous permet de personnaliser leurs fonctionnalités selon vos propres besoins, par exemple en externalisant la recherche de menaces (pour laquelle vous ne disposez peut-être pas de l'expertise requise) tout en mettant en œuvre les fonctionnalités de détection et de réponse au niveau des terminaux en interne.

Qu'en est-il globalement ?

Une fois que vous avez établi vos préférences pour la solution EDR et/ou MDR, vous devrez également évaluer la vision que porte le marché sur les diverses solutions disponibles. Lorsque vous recherchez un produit aussi essentiel que la cybersécurité, les avis des experts indépendants et des utilisateurs existants devraient largement l'emporter sur les affirmations marketing de tout éditeur potentiel. Ainsi, par exemple :



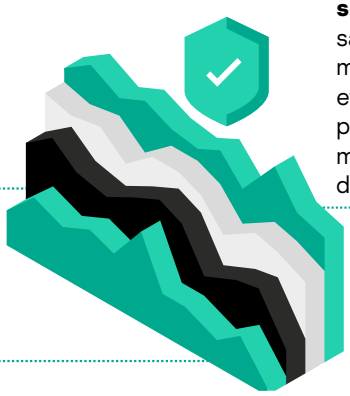
Étape 7 : Tenez compte de votre sécurité dans son ensemble

Dans bon nombre d'entreprises, les solutions EPP, EDR et/ou MDR devront fonctionner au sein d'un cadre de sécurité bien plus large.

En plus de ces solutions, vous pourriez, par exemple, profiter des éléments suivants :

Une mise en sandbox automatisée : ajoute un niveau avancé de détection à vos terminaux en révélant les menaces qui restent dormantes en présence d'une sécurité des terminaux, mais qui s'activent une fois que l'hôte devient vulnérable, et qui doivent donc être analysées dans un environnement contrôle et isolé.

Threat Intelligence : améliore la gestion des problèmes comme les cybermenaces dans les fichiers, URL, IP et domaines suspects et contribue à examiner les menaces plus rapidement et de façon plus minutieuse.



Formation de sensibilisation à la sécurité pour vos salariés : permet de combler les lacunes en matière de sensibilisation à la cybersécurité et de transformer leurs comportements, en particulier compte tenu du fait que la majorité des incidents informatiques sont dus à l'erreur humaine.

Vous devrez également réfléchir aux modalités de gestion de votre solution, par exemple en vous offrant une console unifiée et unique dans le cloud pour tous les différents composants, ce qui inclut les options de gestion Web, sur site et isolées par un espace d'air virtuel (« air gap »).

Étape 8 : Demandez à votre éditeur si son offre inclut tous ces éléments :

Différents éditeurs proposent des solutions EDR et MDR dotées de fonctionnalités variées. En règle générale, une solution complète doit dans l'idéal inclure les éléments suivants :

- Un déploiement rapide et simple
- Des outils faciles d'utilisation et intuitifs qui ne nécessitent pas de longue prise en main ni de nouvelle formation
- Une console de gestion unifiée pour configurer vos outils de cybersécurité et réagir aux incidents depuis un seul emplacement
- Une capacité à répondre à vos exigences et besoins particuliers en choisissant parmi toutes les options de déploiement possibles : dans le cloud, sur site, hybride, air-gapped
- Visibilité des menaces
- Analyse des causes profondes qui inclut des fonctionnalités de visualisation et de recherche approfondie pour des performances plus rapides et pratiques
- Import, génération et analyse d'IoC
- Fonctionnalités de réponse rapide et de préférence automatisée
- Scénarios de réponse à distance
- Recherche de menaces automatisée, prise en charge par l'éditeur /des spécialistes MS(S)P
- Fonctionnalité étroitement intégrée de protection des terminaux, de détection et de réponse au niveau des terminaux
- Fonctionnalité de sandboxing
- Protection intégrée contre les menaces sans fichier
- Technologie contre les vulnérabilités
- Protection contre les ransomwares
- Fonctionnalité de gestion des vulnérabilités et des correctifs
- Contrôle Web, des applications et des appareils, et autres méthodes de renforcement du système
- Performances élevées pour éviter de ralentir les utilisateurs et le réseau
- Support technique efficace dans votre langue

Fonctionnement de Kaspersky Optimum Security

Les résultats des tests indépendants montrent sans équivoque que Kaspersky offre une qualité de protection supérieure à celle des autres éditeurs.

En 2019, pour la troisième année consécutive, nous avons reçu le prix Gartner Peer Insights Customers' Choice pour les plateformes de protection des terminaux[4] , et c'est la septième année consécutive que nous sommes l'éditeur de solutions de sécurité le plus testé et récompensé au monde.

En 2020, nous étions l'un des six éditeurs au monde à recevoir la distinction Gartner Peer Insights Customers' Choice recognition for Endpoint Detection and Response solutions[5], avec la note la plus élevée en termes de service et de support.

Parmi les autres récompenses récemment décernées :

- **Note AA délivrée au produit dans le cadre du test de groupe 2020 NSS Labs Advanced Endpoint Protection (AEP).**
- **Le score le plus élevé possible pour la protection contre les cybermenaces avancées dans le test AV-Comparatives Enhanced Real-World Test.**
- **Prix annuel 2020 SE Labs Best Enterprise Endpoint.**

Kaspersky Optimum Security protège votre entreprise contre les nouvelles menaces, inconnues et évasives, tout en tenant compte des ressources disponibles. Vous pouvez ainsi adopter rapidement et facilement une solution efficace de prévention, de détection et de réponse en matière de menaces, qui s'appuie sur le support des experts Kaspersky pour une surveillance sécurisée 24 h/24, 7 j/7, une recherche de menaces automatisée et des scénarios de réponse à distance guidés.

Si vous recherchez des solutions EPP, EDR et MDR, gérées à partir d'une console dans le cloud et complétées par une sandbox, un portail de Threat Intelligence et une formation de sensibilisation à la sécurité, Kaspersky Optimum Security assure une protection complète à tous vos terminaux dans une solution unifiée qui offre un système de prévention, détection et réponse automatisé, une protection gérée et une formation en cybersécurité.

Protection contre les menaces avancées

- Les mécanismes de prévention et de détection avancées (Machine Learning, analyse comportementale, sandbox, recherche de menaces automatisée avec indicateurs d'attaque (IoA)) optimisent la protection contre les menaces évasives dangereuses reposant sur une forte protection EPP contre les menaces basiques avec Kaspersky Endpoint Security for Business
- La visibilité renforcée des menaces apporte le contexte et les détails des menaces détectées, tandis que les outils de visualisation et d'analyse des causes profondes vous permettent d'enquêter rapidement et efficacement, et de comprendre les menaces et leur mise au point.
- La recherche de menaces automatisée contribue à établir une détection et de réponse des menaces rapide et efficace, par le biais d'une surveillance en continu par des experts leaders du secteur.
- Les options de réponse automatisée rapide sur plusieurs terminaux « en un seul clic » et les analyses d'IoC dans toute l'infrastructure vous permettent de répondre rapidement aux menaces en constante évolution.
- Les scénarios de réponse à distance guidés apportent à vos équipes de sécurité une analyse et des réponses expertes aux menaces nouvelles, inconnues et évasives.
- La sensibilisation des salariés aux cybermenaces, aux méthodes utilisées par les cybercriminels et aux moyens de prévention des attaques réduit les risques d'erreurs humaines et d'ingénierie sociale.

Protection clé en main, rapide et évolutive

- Fonctionne sur l'ensemble des postes de travail, des ordinateurs portables et serveurs, des appareils physiques et virtuels, des clouds publics et des conteneurs.
- La sécurité consolidée des terminaux multi-niveaux hiérarchise les incidents et accélère la découverte et l'enquête des menaces avec la Threat Intelligence via un portail Web simple à utiliser.
- Mettez fin aux menaces connues et émergentes en utilisant des technologies performantes qui ont fait leurs preuves dans la prévention des ransomwares, des vulnérabilités, des attaques de logiciels sans fichiers et d'autres programmes malveillants.

4 Gartner Peer Insights 'Voice of the Customer': Endpoint Protection Platforms, 10 Décembre 2019
5 Gartner Peer Insights 'Voice of the Customer': Endpoint Detection and Response Solutions, 1er mai 2020

Gartner Peer Insights Customers' Choice est le reflet d'avis subjectifs provenant d'évaluations, de classements et de données d'utilisateurs finaux individuels, appliqués à une méthodologie documentée. Il ne reflète pas le point de vue de Gartner ou ses sociétés affiliées ni ne constitue une approbation de leur part.

Diminue les besoins en personnel ou d'expertise supplémentaire

- Les processus d'analyse et de réponse simples au sein d'une console unique dans le cloud permettent au personnel de sécurité d'optimiser le temps et les efforts consacrés à l'enquête et à la résolution.
- Une console unifiée facilite l'administration unique des principales application de sécurité Kaspersky. On peut configurer les outils de cybersécurité et les faire réagir aux incidents depuis un seul emplacement. Ils peuvent répondre à des besoins particuliers en choisissant parmi toutes les options de déploiement possibles : dans le cloud, sur site, hybride et avec isolement par un espace d'air virtuel (air-gapped).
- Une surveillance sécurisée 24 h/24, 7 j/7 assure une protection en continu, y compris pour les organisations manquant de personnel de sécurité informatique.

Pourquoi investir dans Kaspersky Optimum Security

Kaspersky Optimum Security vous fera passer d'un risque considérable d'attaque évasive à une confiance renouvelée en votre sécurité des terminaux. Au lieu de ne pas savoir exactement ce qui se passe dans votre environnement, vous aurez une visibilité et un contrôle sur tous vos terminaux, où qu'ils soient. Et plutôt que de rechigner à mettre à niveau la sécurité pour des raisons de complexité, vous disposerez d'une solution simplifiée et consolidée qui optimisera vos ressources.

Pour une protection avancée tout en diminuant le recours à des ressources supplémentaires, rendez-vous sur **https://kas.pr/optim-edr**.

Actualités sur les cybermenaces : www.securelist.com
Actualités sur la sécurité informatique : www.kaspersky.fr/blog
Portail de Threat Intelligence : opentip.kaspersky.com
Technologies en bref : www.kaspersky.fr/enterprise-security/wiki-section/home
Récompenses : www.kaspersky.fr/enterprise-security#awards
Catalogue interactif : www.kaspersky.com/int_portfolio/fr

www.kaspersky.fr

kaspersky BRING ON THE FUTURE