kaspersky PRÊTS POUR L'AVENIR

Kaspersky Endpoint Detection and Response Optimum

Faites passer vos défenses de terminaux à la vitesse supérieure et affrontez les menaces évasives de plein fouet et en toute tranquilité.

Il est temps de passer à la vitesse supérieure. Vous êtes prêt non seulement à protéger votre organisation avec des technologies traditionnelles de protection contre les programmes malveillants, mais aussi à identifier, analyser et neutraliser efficacement ces menaces délibérément conçues pour échapper à la protection traditionnelle et s'enfouir profondément dans vos systèmes, disposées à engendrer d'énormes dégâts.

Des outils système légitimes sont utilisés dans environ **30 % des attaques réussies** pour lancer des scripts et des programmes, télécharger des charges utiles, analyser des réseaux ou obtenir un accès à distance à l'hôte infecté.
Rapport analytique concernant les réponses aux incidents, Kaspersky, 2020

Les défis

Perturbations affolantes

Les logiciels malveillants, les ransomwares, les logiciels espions financiers et d'autres menaces échappent de plus en plus à la détection et l'élaboration des attaques est toujours moins chère. Le risque d'une attaque sérieuse est ainsi plus conséquent que jamais, tout comme les niveaux de dommages et de perturbations impliqués.

Infrastructures complexes

De nos jours, la plupart des responsables informatiques et des professionnels de la sécurité doivent protéger une gamme complète de terminaux différents : ordinateurs portables, serveurs, environnements virtuels et cloud de même que des postes de travail distants, tout en faisant face à des systèmes informatiques à la complexité à peine maîtrisable.

Trouver l'équilibre

La cybersécurité consiste principalement à trouver l'équilibre optimal entre vos ressources disponibles et le plus haut niveau de protection que l'on peut raisonnablement escompter. Par ailleurs, le temps de votre informaticien est l'une des ressources les plus rares et précieuses de toutes.

Même lors d'attaques réussies, les pertes financières étaient **inférieures de 32 %** si l'on réagissait à une violation rapidement.
Rapport analytique concernant les réponses aux incidents, Kaspersky, 2020

La réponse

Kaspersky Endpoint Detection and Response (EDR) Optimum vous aide à identifier, analyser et neutraliser les menaces évasives en fournissant une détection avancée facile à utiliser, une investigation simplifiée et une réponse automatisée.

Une préparation complète armés jusqu'aux dents

Kaspersky EDR Optimum vous offre une visibilité approfondie sur les menaces, des outils d'analyse et d'investigation simples avec une réponse automatisée en fonction des mécanismes de détection avancés, notamment l'apprentissage automatique et l'analyse comportementale améliorée. Vous allez être en mesure de détecter la menace, de la comprendre, de révéler toute sa portée et de réagir instantanément, évitant ainsi toute interruption de votre activité.

Une solution unique

Kaspersky EDR Optimum apporte des capacités avancées de détection, d'analyse et de réponse à l'écosystème de sécurité Kaspersky, améliorant les défenses sur une gamme complète de terminaux, notamment les ordinateurs portables, les serveurs, les charges de travail dans le cloud et les environnements virtuels. Le déploiement centralisé et la gestion unifiée de Kaspersky EDR Optimum sont disponibles depuis le cloud ou sur site.

Simple et efficace

Kaspersky EDR Optimum est conçu pour les petites équipes de cybersécurité aux moyens limités qui cherchent à mettre à niveau leurs capacités de réponse aux incidents. Les performances sont optimisées pour une efficacité maximale avec une intervention humaine minimale, tirant parti au maximum du temps de vos spécialistes de la sécurité grâce à l'automatisation et la centralisation de tous les flux de travail d'administration et de rationalisation.

Principaux avantages

- Protégez-vous contre les menaces évasives plus fréquentes et plus perturbatrices
- Défendez chaque terminal : ordinateurs portables, serveurs, charges de travail dans le cloud
- Visualiser l'ampleur de n'importe quelle menace sur l'intégralité du réseau
- Comprendre les causes profondes de la menace et son origine
- Éviter des dommages préjudiciables par le biais d'une réponse rapide et automatisée
- Gagner du temps et des ressources grâce à un outil automatisé et simplifié

Cas d'utilisation EDR décisifs

Détection avancée

Une détection avancée est nécessaire afin de découvrir les menaces évasives :

- Détection des menaces comportementales et prévention des exploitations des failles de sécurités optimisées par l'apprentissage automatique (ML - Machine Learning)
- Méthodes heuristiques, enregistrements intelligents, technologies fondées sur le ML
- Émulateur intégré pour la prédétection des comportements malveillants
- Sandbox pour une analyse comportementale améliorée (disponible avec Kaspersky Sandbox)
- Données mondiales de renseignements sur les menaces collectées et analysées en laboratoire par des systèmes et des experts reposants sur l'IA

Répondre à des questions vitales

Les menaces évasives se cachent souvent en pleine lumière et doivent faire l'objet d'une enquête pour être totalement éradiquées. EDR vous permet de trouver les réponses à ces questions :

- Suis-je attaqué en ce moment ?
- Cette attaque à l'échelle de l'industrie a-t-elle atteint mon infrastructure ?
- D'où provient cette menace ?
- Qu'a-t-elle parvenu à faire sur mes hôtes ?
- Y a-t-il des couches dissimulées à cette menace ?
- D'autres terminaux sont-ils affectés ?

Répondre rapidement

Répondez aux menaces en un seul clic ou avec une réponse automatisée dès leur découverte :

- Empêcher le fichier malveillant de s'exécuter et de se propager à travers le réseau durant ou après votre investigation
- Isoler automatiquement les fichiers associés à des menaces évasives sur tous les terminaux
- Isoler automatiquement les hôtes infectés dès la découverte d'un Indicateur de compromission (IoC) lié à une menace prolifique

Vous pouvez désormais accomplir tellement plus

À présent, vous pouvez comprendre la portée intégrale de toute menace qui vous attaque et comment elle se développe sur vos terminaux, en tirant parti de la détection avancée reposant sur l'apprentissage automatique et de la visibilité concernant les détections. De même, vous pouvez vous assurer que chaque menace a été entièrement traitée : plus rien ne s'enfonce quelque part à l'intérieur de votre système, en calculant les dangers éventuels.

Défendre des infrastructures hybrides

Les infrastructures hybrides présentent tout aussi bien des défis de sécurité uniques que des avantages significatifs. Vous pouvez dès à présent améliorer la protection de vos données et de votre infrastructure pour les serveurs virtuels et physiques, les déploiements VDI et les charges de travail dans le cloud public avec des fonctionnalités EDR fondamentales.

Évitez une baisse de la vigilance par rapport aux alertes et mettez pleinement à profit vos ressources avec une gestion centralisée de tous vos terminaux et charges de travail hybrides et un flux de travail EDR rationalisé depuis le cloud ou sur site.

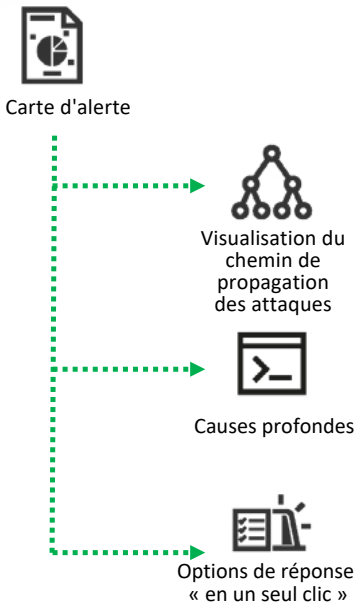
Protection des terminaux à différents niveaux

Les technologies EDR n'existent pas dans le vide : elles ne peuvent fonctionner efficacement qu'à partir d'une solide base de protection des terminaux. La protection des terminaux à plusieurs niveaux garantit que vous n'êtes pas distrait par la gestion des menaces et des incidents qui auraient dû être traités au préalable par un logiciel automatisé de protection contre les programmes malveillants. C'est la raison pour laquelle Kaspersky EDR Optimum fonctionne avec l'une de nos plateformes de protection des terminaux les plus éprouvées et les plus primées[1] : Kaspersky Endpoint Security for Business et Kaspersky Hybrid Cloud Security.

Analyser les menaces

Dans une seule et même carte d'incident, des données enrichies sur la détection et un chemin de propagation d'attaque détaillé sont rassemblés afin d'effectuer une analyse rapide et prendre des décisions éclairées pour une réponse automatisée ou en un seul clic.

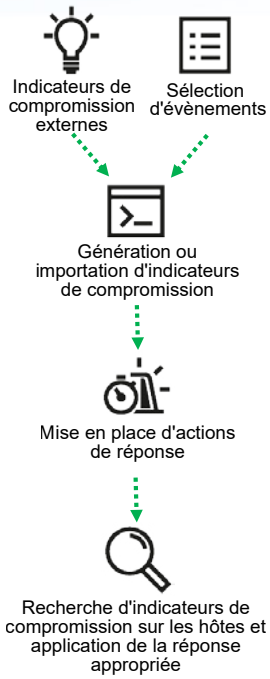
Les IoC peuvent être importés à partir de sources de confiance ou générés en fonction de l'enquête afin de découvrir les menaces évasives qui se cachent sur les terminaux de votre infrastructure.



Automatisez votre réponse

Répondez instantanément aux menaces au cours de l'investigation avec les options « en un seul clic » disponibles dans la carte d'incident ou configurez des réponses automatisées lors de la découverte selon les analyses IoC. Les actions de réponse sont notamment :

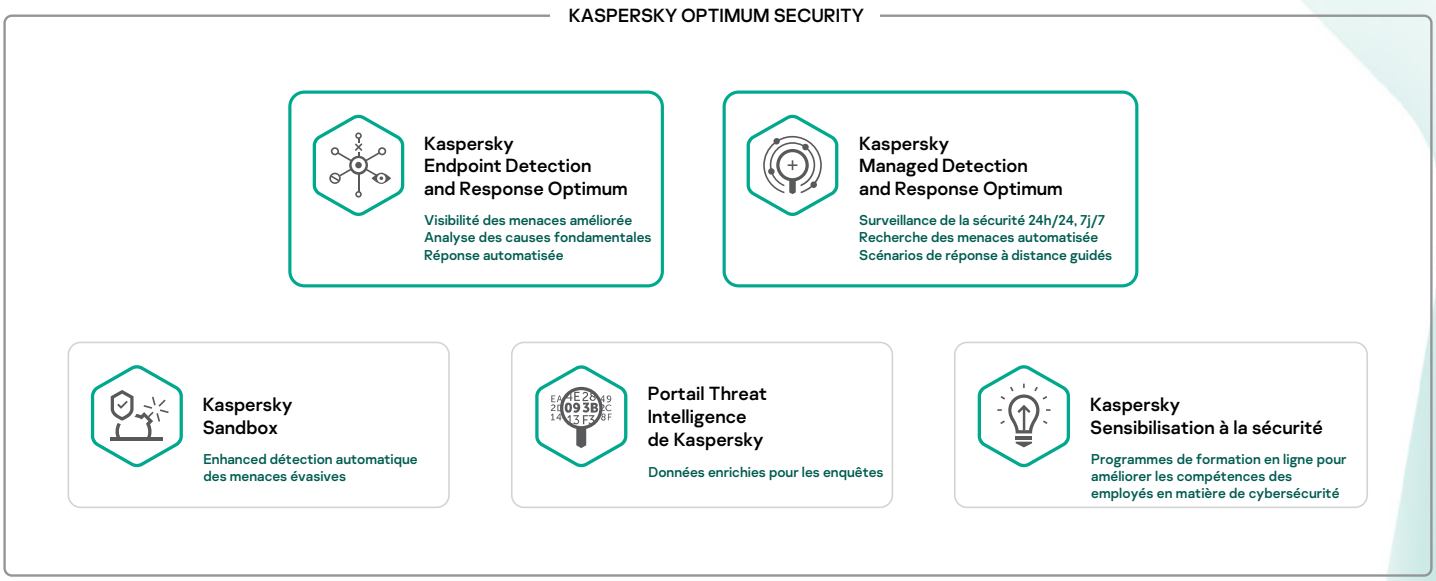
- Isoler l'hôte
- Mettre des fichiers en quarantaine
- Prévenir son exécution
- Lancer l'analyse des zones critiques



[1] https://www.kaspersky.co.uk/top3

Votre plateforme Kaspersky Optimum Security

EDR fait partie d'un écosystème couvrant une multitude de technologies, outils et services : Kaspersky EDR Optimum est un composant clé de Kaspersky Optimum Security, une solution à plus vaste échelle renforçant plusieurs aspects de vos défenses contre les menaces évasives, sans oublier de ménager vos ressources :



L'approche par étape en matière de cybersécurité

Kaspersky Optimum Security repose sur Kaspersky Security Foundations. Au moment où vous êtes prêt à le faire et si vous l'êtes, vous pouvez avec Kaspersky Expert Security choisir de passer de manière harmonieuse à l'application d'outils performants qui protègent contre les menaces les plus avancées.

Kaspersky Security Foundations

Bloquez automatiquement la grande majorité des menaces.

- La prévention automatisée multivecteur des incidents causés par des menaces primaires : la grande majorité des cyberattaques
- L'étape de base pour les organisations de toute taille et complexité dans l'élaboration d'une stratégie de défense intégrée
- Une protection fiable des terminaux pour ceux qui disposent de petites équipes informatiques et une expertise émergente en matière de sécurité

Kaspersky Optimum Security

Renforcez vos défenses contre les menaces évasives. Cette solution est adaptée aux profils suivants :

- Les entreprises qui disposent d'une petite équipe de sécurité informatique ayant une expertise de base en matière de cybersécurité
- Les entreprises qui disposent d'un environnement informatique dont la taille et la complexité évoluent, ce qui élargit la surface d'attaque
- Les entreprises qui manquent de ressources en matière de cybersécurité, mais qui ont besoin d'une protection renforcée
- Les entreprises qui ont besoin croissant de développer une capacité de réponse aux incidents

Kaspersky Expert Security

Assurez une protection contre les attaques complexes et de type APT à plusieurs niveaux. Cette solution est adaptée aux entreprises avec les profils suivants :

- Environnements informatiques complexes et distribués
- Une équipe de sécurité informatique mature ou un Centre d'opérations de sécurité (SOC) établi
- Les entreprises qui ont une aversion pour le risque en raison des coûts plus élevés des incidents de sécurité et des violations de données
- Mais aussi celles qui se préoccupent du respect des réglementations

Pour en savoir plus sur la manière dont Kaspersky Endpoint Detection and Response Optimum traite les cybermenaces tout allégeant la charge de travail de votre équipe de sécurité et les ressources, rendez-vous sur le site http://www.kaspersky.com/enterprise-security/edr-security-software-solution.

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com

www.kaspersky.fr