kaspersky PRÊTS POUR L'AVENIR

Kaspersky Endpoint Detection and Response

Érigez une véritable défense en profondeur, avec une réponse automatisée instantanée et une analyse des causes profondes simplifiée

La problématique

91 % des organisations ont été affectées par des cyberattaques en 2019, parmi lesquelles **1 sur 10** a dû faire face à une attaque ciblée[1].

Les menaces complexes génèrent des perturbations

Le temps des programmes malveillants simplistes est révolu depuis longtemps. Les menaces sont devenues bien plus sophistiquées, générant davantage de perturbations et de pertes pour les entreprises, tout en restant dissimulées pendant plus longtemps.

Votre entreprise est attaquée

Ces menaces complexes sont aujourd'hui moins chères à mettre en œuvre et plus fréquentes. Ainsi, les organisations qui se pensaient intouchables doivent maintenant couvrir leurs arrières.

L'efficacité est un impératif

De plus, les organisations doivent faire face à un manque de ressources, dont deux figurant parmi les plus précieuses : le temps et le personnel qualifié.

Nos solutions pour y faire face

« Une solution Endpoint faible détruira la valeur d'un outil EDR »[2]

« Le personnel et le temps deviennent le nouvel indicateur de retour sur investissement pour les outils EDR »[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum vous protège contre les menaces complexes et avancées au moyen d'une détection avancée, d'une investigation simplifiée et d'une réponse automatisée.

Au-delà des fonctionnalités essentielles

Bénéficiez d'une grande visibilité, d'outils d'investigation simplifiés et d'options de réponse automatisée, afin de ne pas simplement détecter la menace, mais d'identifier son ampleur et ses origines, et d'y répondre instantanément. Vous empêcherez ainsi toute perturbation de votre activité.

Une véritable défense en profondeur

Découvrez un kit d'outils de détection et de réponse convivial et hautement automatisé, associé aux fonctionnalités inégalées de détection avancée et de protection des terminaux de Kaspersky Endpoint Security for Business, au sein d'une offre unifiée.

Un outil intelligent pour une efficacité garantie

Libérez votre temps, tout en optimisant vos ressources et vos frais informatiques, grâce à des contrôles centralisés simplifiés et un niveau élevé d'automatisation. Rationalisez votre flux de travail à partir d'une console unique, disponible pour les configurations sur site comme dans le cloud[3].

Principaux avantages

- Vous protéger contre les menaces avancées et complexes les plus fréquentes et les plus perturbatrices
- Gagner du temps et des ressources grâce à un outil automatisé et simplifié
- Visualiser l'ampleur des menaces complexes sur l'intégralité du réseau
- Comprendre les causes profondes de la menace et la façon dont elle a pénétré dans votre périmètre
- Éviter des dommages préjudiciables par le biais d'une réponse rapide et automatisée

Cas d'utilisation de l'EDR

Répondez aux questions essentielles

- Quel est le contexte de l'alerte ?
- Quelles actions ont déjà été mises en œuvre à la suite de l'alerte ?
- La menace détectée est-elle toujours active ?
- D'autres hôtes sont-ils attaqués ?
- Quel chemin l'attaque a-t-elle emprunté ?
- Quelles sont les véritables causes profondes de la menace ?

Faites état de l'ampleur de la menace

Dès que vous apprenez qu'un risque de menace globale pèse sur votre entreprise (par ex., si les autorités réglementaires vous demandent d'exécuter l'analyse d'un indicateur de compromission [IoC] spécifique), vous pouvez :

- Importer des IoC issus de sources fiables et exécuter des analyses périodiques pour identifier tout signe d'attaque
- Examiner une alerte en détails, créer des IoC basés sur les menaces identifiées et exécuter des analyses sur l'intégralité du réseau afin de découvrir si d'autres hôtes ont été infectés

Répondre instantanément aux menaces prolifiques

- Isoler automatiquement les fichiers associés aux menaces complexes sur tous les terminaux
- Isoler automatiquement les hôtes infectés dès la découverte d'un IoC associé à une menace prolifique
- Empêcher le fichier malveillant de s'exécuter et de se propager à travers le réseau durant votre investigation

[1] Le rapport Kaspersky sur les risques informatiques mondiaux, Kaspersky, 2019

[2] IDC, Sécurité des terminaux 2020 : La résurgence de la protection des terminaux et le destin de l'EDR, Doc n° US45794219, 2020

[3] Les caractéristiques et fonctionnalités pouvant être gérées via la console cloud font l'objet de certaines restrictions. Pour plus d'informations, rendez-vous sur https://help.kaspersky.com/KSC/CloudConsole/fr-fr/195507.htm

Maintenant, vous pouvez :

Visualiser l'ampleur de la menace

Visualisez les alertes de sécurité sur vos terminaux et menez une analyse approfondie afin de comprendre l'étendue et la profondeur de la menace. Cela permet de garantir que les incidents sont traités de bout en bout et qu'aucune menace résiduelle ne demeure sur le terminal.

Simplifier votre flux de travail

Un flux de travail rationalisé à partir d'une console unique, disponible pour les configurations sur site comme dans le cloud, est associé à des scénarios et contrôles EDR simplifiés, notamment la visualisation des détails, l'analyse des IoC et les options de réponse qui ne nécessitent pas un temps ni une expertise en cybersécurité démesurés.

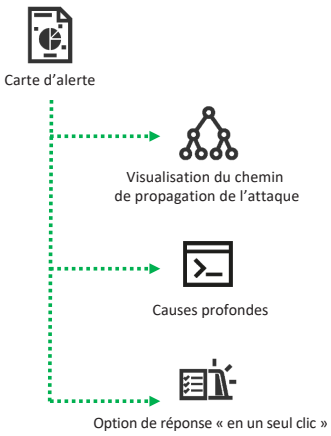
Rebooster votre défense

L'ajout de Kaspersky Sandbox crée une solution intégrée de sécurité des terminaux complète, qui offre une défense multi-niveaux simple, efficace et hautement automatisée contre les menaces classiques, complexes et difficilement détectables.

Analyser des données exhaustives sur l'alerte

Kaspersky EDR Optimum vous renseigne sur les incidents et vous aide à comprendre les connexions entre divers évènements à travers la visualisation du chemin de l'attaque.

La solution vous apporte une visibilité sur l'ensemble des hôtes du réseau en analysant les indicateurs de compromission (IoC) importés ou créés.



Répondre de façon automatisée

Paramétrez des réponses automatisées aux menaces identifiées sur l'ensemble des terminaux sur la base des analyses des IoC, ou répondez instantanément aux incidents à l'aide des options « en un seul clic ».

Options de réponse incluses : isoler un hôte ou un fichier, lancer l'analyse d'un hôte et empêcher l'exécution d'un fichier.

D'autres options EDR

Kaspersky Endpoint Detection and Response Optimum est l'une des nombreuses solutions EDR que nous proposons. Chacune d'entre elles est conçue pour répondre à des besoins spécifiques. Cela peut également vous intéresser :

Kaspersky Endpoint Detection and Response

Cette solution EDR, reconnue parmi les experts du secteur et nos clients, est idéale pour les organisations informatiques disposant d'équipes de sécurité informatique matures. Elle contribue à élucider les attaques ciblées et avancées les plus sophistiquées. Parmi ses atouts figurent l'identification avancée des menaces, de puissantes fonctionnalités d'investigation, la recherche proactive des menaces et la réponse centralisée aux incidents.
https://www.kaspersky.fr/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Basée sur une expertise des menaces de plus de 20 ans, cette solution aux fonctions de détection, de priorisation, d'investigation et de réponse entièrement gérées et personnalisées 24 h/24, 7 j/7 vous permet de bénéficier des principaux avantages d'un SOC sans devoir en créer un.
https://www.kaspersky.fr/enterprise-security/managed-detection-and-response

Pour en savoir plus sur la façon dont Kaspersky Endpoint Detection and Response Optimum traite les cybermenaces, tout en limitant l'intervention de votre équipe de sécurité et de vos ressources, rendez-vous sur
http://www.kaspersky.fr/enterprise-security/edr-security-software-solution

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les entreprises : https://www.kaspersky.fr/enterprise-security
Kaspersky Threat Intelligence Portal : opentip.kaspersky.com

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Proven. Transparent. Independent.