Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

Les cybercriminels utilisent des techniques de plus en plus sophistiquées et sont capables de contourner efficacement les protections existantes. Chaque secteur de votre entreprise peut être exposé à des risques, ce qui perturbe les processus critiques de l'entreprise, nuit à la productivité et augmente les coûts d'exploitation.

Avec Kaspersky EDR, votre entreprise peut :

- **SURVEILLER** efficacement les menaces ne se limitant pas aux programmes malveillants
- **DÉTECTER** précisément les menaces à l'aide de technologies avancées
- Centraliser l'**AGGRÉGATION** des données brutes et des résultats
- **RÉPONDRE** rapidement aux attaques
- **EMPÊCHER** les actions malveillantes issues des menaces détectées...

... le tout sur une interface Web intuitive, simplifiant les opérations d'enquête et de réponse.

Kaspersky EDR et les principales conclusions du rapport Endpoint Security 2020 d'IDC*

- **Une solution EPP faible détruit la valeur d'un outil EDR**

  Kaspersky offre des protections complètes et puissantes des terminaux (EPP+EDR) via un seul agent

- **Le personnel et le temps deviennent le nouvel indicateur de retour sur investissement pour les outils EDR**

  Kaspersky automatise considérablement les problèmes complexes, ce qui permet à vos experts en sécurité de gagner un temps précieux

- **L'EDR doit exploiter les données qui se trouvent en dehors des terminaux**

  Kaspersky renforce l'efficacité de l'EDR en ajoutant un outil unique de visibilité et de détection avancées des menaces transmises par email et par le Web

Renforcer d'abord votre protection au niveau des terminaux

Les terminaux d'entreprise, où les données, les utilisateurs et les systèmes d'entreprise se rassemblent pour générer et mettre en œuvre des processus commerciaux, restent la cible principale de cybercriminels. Pour protéger vos terminaux d'entreprise et éviter qu'ils soient utilisés comme points d'entrée pour attaquer votre infrastructure, votre équipe experte en cybersécurité doit chercher à améliorer votre sécurité existante. Depuis le blocage automatique des menaces courantes jusqu'à une réponse rapide et appropriée face à des incidents complexes, la mise en œuvre du cycle complet de protection des terminaux nécessite des technologies de prévention complétées par des fonctionnalités avancées de protection.

Kaspersky Endpoint Detection and Response (EDR) offre une sécurité efficace, une visibilité complète sur tous les terminaux du réseau de l'entreprise ainsi que des systèmes de défense avancés, permettant l'automatisation des tâches de routine afin de détecter, hiérarchiser, examiner et neutraliser les menaces les plus sophistiquées et les attaques de type APT.

Bénéfices

- Kaspersky EDR améliore **Kaspersky Endpoint Security for Business**, notre plateforme phare Endpoint Protection Platform (EPP) la plus testée et la plus primée, avec de puissantes fonctionnalités EDR, renforçant encore vos niveaux de sécurité globaux. Un agent unique pour une protection automatisée contre les menaces actuelles et des systèmes de protection avancés contre les attaques complexes simplifient la gestion des incidents et minimisent les besoins de maintenance. Il n'y a aucune charge supplémentaire au niveau des terminaux ni aucun coût supplémentaire, juste la certitude que vos postes de travail et vos serveurs sont efficacement protégés contre les menaces les plus sophistiquées et les attaques ciblées.
- Kaspersky EDR réduit le temps nécessaire pour collecter les preuves initiales, fournit une analyse télémétrique complète et maximise l'automatisation des processus EDR, réduisant ainsi le temps de réponse global aux incidents sans qu'il soit nécessaire de faire appel à des ressources supplémentaires en matière de sécurité informatique.
- Kaspersky EDR peut être intégré à la plateforme **Kaspersky Anti Targeted Attack**, associant les fonctionnalités EDR et la détection avancée des menaces au niveau du réseau. Les experts en sécurité informatique disposent de tous les outils nécessaires pour gérer la détection de menaces multidimensionnelles supérieures, tant au niveau des terminaux que des réseaux. Pour cela, ils peuvent utiliser des technologies de pointe, mener des enquêtes efficaces et réagir de manière rapide et centralisée, le tout grâce à une solution unique.

* IDC PERSPECTIVE, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR
(IDC, Sécurité des terminaux 2020 : La résurgence de la protection des terminaux et la destinée manifeste de l'EDR)

Kaspersky EDR est une solution idéale si votre organisation souhaite :

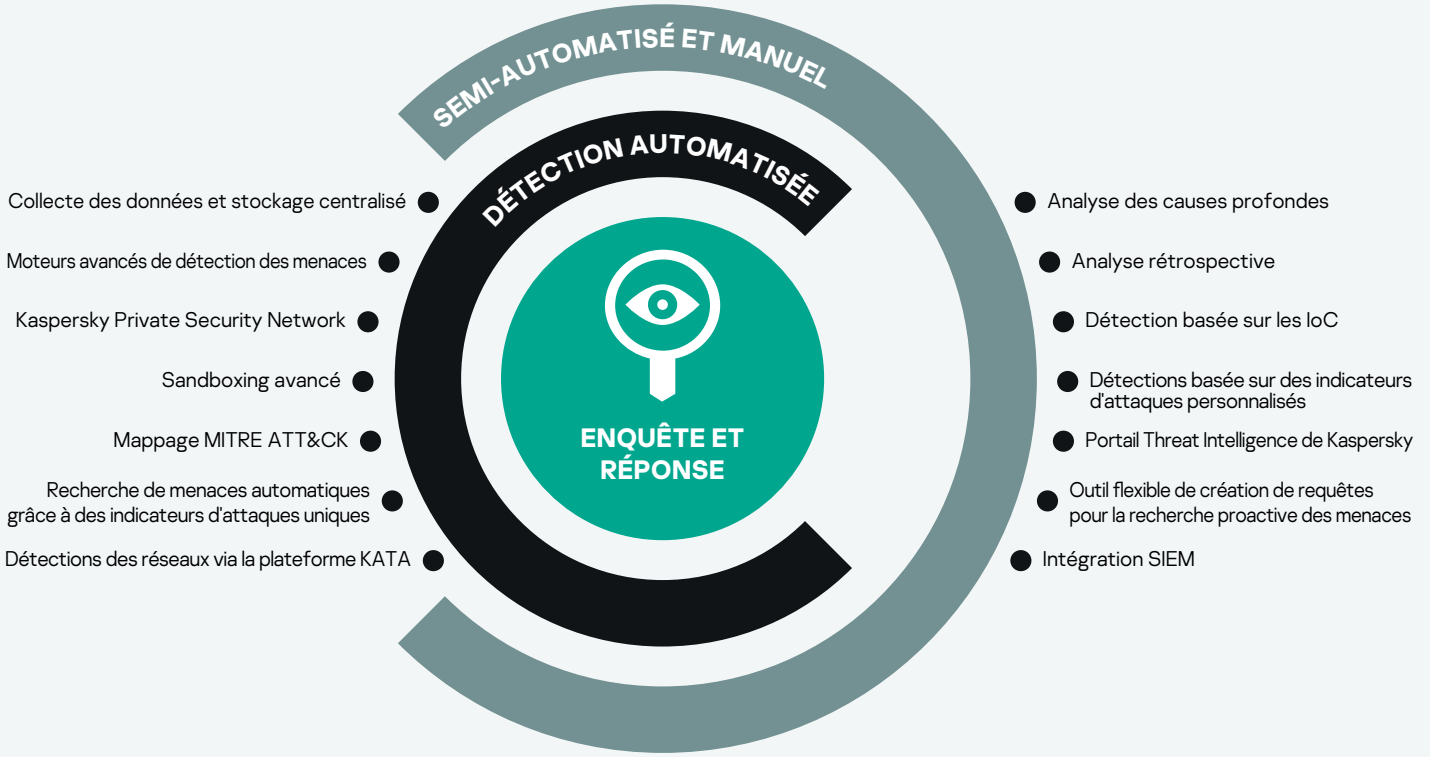
- Renforcer la sécurité grâce à une solution d'entreprise de réponse aux incidents facile à utiliser
- Automatiser la détection des menaces et les réponses à celles-ci, le tout sans perturber les activités pendant les enquêtes
- Améliorer la visibilité de vos terminaux et la détection des menaces grâce à des technologies avancées
- Comprendre les tactiques, les techniques et les procédures (TTP) particulières employées par les auteurs de menaces pour atteindre leurs objectifs, ce qui permet d'améliorer l'efficacité de la protection ainsi que l'allocation des ressources en matière de sécurité
- Établir des processus unifiés et efficaces de recherche des menaces, de gestion des incidents et de réponse
- Augmenter l'efficacité de votre centre d'opérations de sécurité interne : ne perdez pas de temps à analyser des journaux de terminaux non pertinents
- Assurer la conformité en mettant en place des journaux de terminaux, des avis d'alerte et la documentation des résultats d'enquêtes

Découvrir et contenir rapidement les menaces les plus sophistiquées

Kaspersky EDR assure une protection des terminaux de haut niveau et augmente l'efficacité du centre d'opérations de sécurité en permettant une détection avancée des menaces et en donnant accès à des données rétrospectives, même dans des situations où les terminaux compromis sont inaccessibles ou lorsque les données ont été chiffrées au cours d'une attaque. Des possibilités d'enquête renforcées grâce à nos indicateurs d'attaque (IoA) uniques, à l'enrichissement de la base MITRE ATT&CK et à un outil flexible de création de requêtes ainsi qu'à l'accès à notre base de connaissances du portail Threat Intelligence Portal. Tous ces éléments permettent de rechercher les menaces de manière efficace et de réagir rapidement aux incidents, ce qui contribue à limiter et à prévenir les dégâts.

Cas d'utilisation :

- **Recherche proactive de preuves d'intrusion sur l'ensemble de votre réseau**
- **Détection et résolution rapide des intrusions, avant qu'elles ne causent des interruptions et des dégâts majeurs**
- **Enquête rapide et gestion centralisée des incidents sur des milliers de terminaux par le biais d'un flux de travail parfaitement intégré**
- **Validation des alertes et des incidents potentiels détectés par d'autres solutions de sécurité**
- **Automatisation des opérations de routine, afin de réduire les tâches manuelles, de libérer vos ressources et d'éviter la « surcharge d'alerte »**



Gartner peerinsights customers' choice 2020™

Le Gartner Peer Insights Customers' Choice pour les solutions EDR 2020 désigne Kaspersky comme le meilleur fournisseur

Kaspersky est l'un des six seuls fournisseurs au monde à être reconnu par le Gartner Peer Insights Customers' Choice pour sa solution Endpoint Detection and Response en 2020. Celle-ci a obtenu la classification la plus élevée parmi tous les fournisseurs pour son service et son assistance. Il s'agit donc du témoignage ultime de la reconnaissance des clients de Kaspersky EDR.

Décharge de responsabilité de Gartner

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.

MITRE | ATT&CK®

Qualité de la détection confirmée par l'évaluation MITRE ATT&CK

En reconnaissance de l'importance de l'analyse TTP (tactiques, techniques et procédures) dans les investigations sur les incidents complexes et le rôle de MITRE ATT&CK sur le marché de la sécurité aujourd'hui :

- Kaspersky EDR a participé à la phase 2 de l'évaluation MITRE (APT29) et a démontré des performances élevées dans la détection des principales techniques ATT&CK de la phase 2 appliquées à des étapes cruciales d'attaques ciblées modernes
- Les détections de Kaspersky EDR sont enrichies de données issues de la base de connaissances MITRE ATT&CK, ce qui permet d'analyser en profondeur les TTP de votre adversaire.

Pour en savoir plus, rendez-vous sur kaspersky.fr/MITRE

Avantages commerciaux de Kaspersky EDR dans toute l'entreprise :

- Élimination des failles de sécurité et réduction des temps d'arrêt dus aux attaques
- Automatisation des tâches manuelles pendant la détection des menaces et l'intervention
- Allègement de la charge de travail du personnel des services informatiques, lui permettant de se consacrer à d'autres tâches essentielles
- Simplification de l'analyse des menaces et de la réponse aux incidents
- Réduction du temps nécessaire à la détection et au blocage des menaces
- Mise en conformité totale

Et si vous en voulez encore plus… Kaspersky Managed Detection and Response

L'ajout à Kaspersky EDR d'un système de défense 24 heures sur 24 entièrement géré et personnalisé permet de préserver vos ressources en matière de sécurité informatique en confiant à Kaspersky les tâches de traitement des incidents ou en faisant appel à nous pour obtenir des avis d'experts et une expertise unique en matière de recherche des menaces lorsque votre équipe interne ne dispose pas de spécialistes en sécurité suffisamment qualifiés pour faire face à des scénarios particuliers.

Pour en savoir plus sur Kaspersky EDR, consultez le site suivant :

kaspersky.fr/enterprise-security/endpoint-detection-response-edr

Actualités sur les cybermenaces : securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

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.

Pour en savoir plus, rendez-vous sur kaspersky.fr/transparency

Proven. Transparent. Independent.