kaspersky BRING ON THE FUTURE*

Kaspersky Managed Detection and Response

Face aux incidents de cybersécurité, la plupart des équipes de sécurité adoptent une approche fondée sur les alertes et n'interviennent qu'une fois que l'incident s'est produit. Pendant ce temps, les nouvelles menaces échappent aux radars, donnant littéralement un faux sentiment de sécurité. Les entreprises sont de plus en plus nombreuses à reconnaître la nécessité de rechercher proactivement les menaces non détectées, mais pourtant actives au sein de leurs infrastructures.

Avantages du produit :

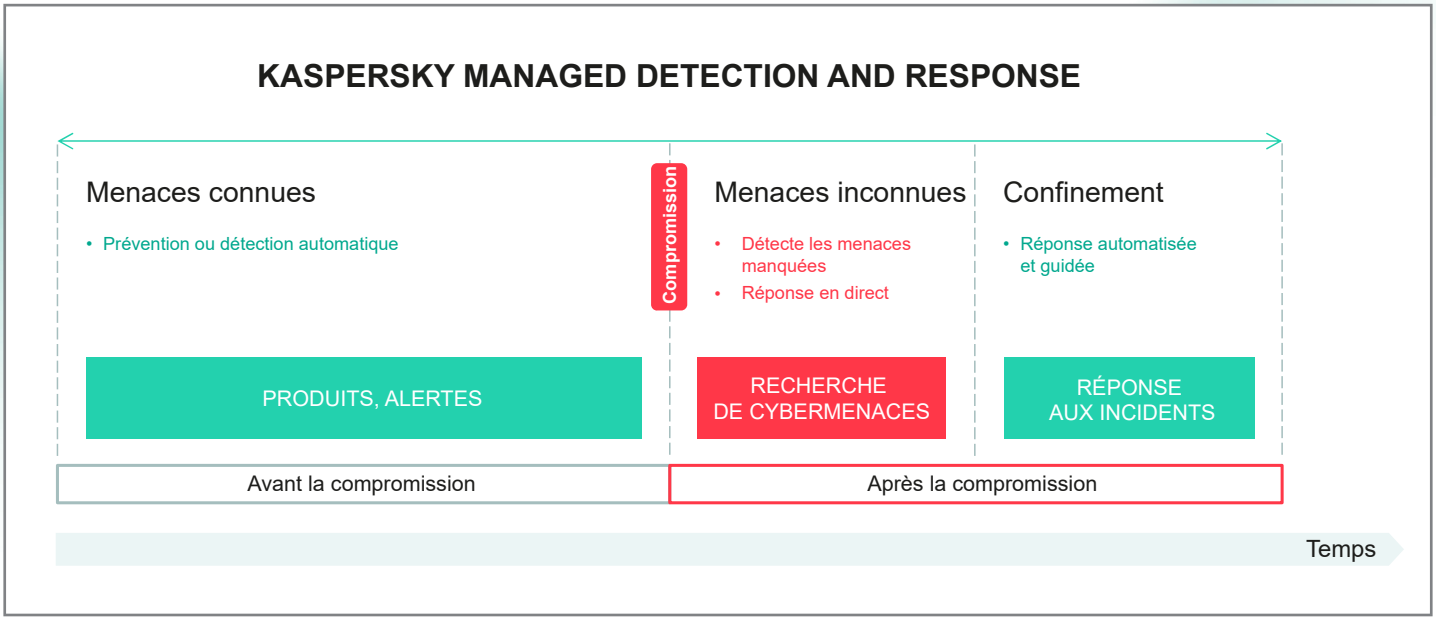
- La certitude rassurante d'être protégé en permanence, même contre les menaces les plus innovantes
- Une réduction du coût total relatif à la sécurité, en supprimant le besoin d'employer un large éventail de spécialistes dédiés en interne
- La possibilité de consacrer les ressources internes onéreuses aux tâches critiques qui en ont réellement besoin
- Tous les principaux avantages d'un centre de sécurité (SOC) sans même devoir en créer un

Kaspersky Managed Detection and Response (MDR) fournit une protection avancée 24 heures sur 24 contre le volume grandissant de menaces qui contournent les barrières de sécurité automatisées, soulageant ainsi les organisations qui peinent à trouver du personnel spécialisé ou qui disposent de ressources limitées en interne.

Ses fonctionnalités avancées de détection et de réponse s'appuient sur l'une des équipes de recherche de menaces les plus efficaces et expérimentées du secteur. Contrairement aux solutions similaires présentes sur le marché, Kaspersky MDR est basée sur des modèles de Machine Learning brevetés, une Threat Intelligence continue et unique et une expérience éprouvée de recherche efficace sur les attaques ciblées. Cette solution renforce automatiquement la résilience de votre entreprise face aux cybermenaces, tout en optimisant vos ressources existantes et vos futurs investissements de sécurité informatique.

Caractéristiques principales du produit

- Un déploiement clé en main, rapide et évolutif, permettant d'obtenir une sécurité informatique mature instantanément sans qu'il soit nécessaire d'investir dans du personnel ou des compétences supplémentaires
- Une protection supérieure, même contre les menaces d'origine non malveillante les plus complexes et les plus innovantes, afin d'empêcher les interruptions d'activité et de réduire l'impact général des incidents
- Une réponse entièrement gérée ou guidée aux incidents, permettant une réaction rapide tout en gardant le contrôle total de toutes les actions
- Une visibilité en temps réel sur toutes les ressources et leur statut de protection, assurant une connaissance situationnelle permanente à travers divers canaux de communication



Graphique 1. KASPERSKY MANAGED DETECTION AND RESPONSE

*Bienvenue dans le futur.

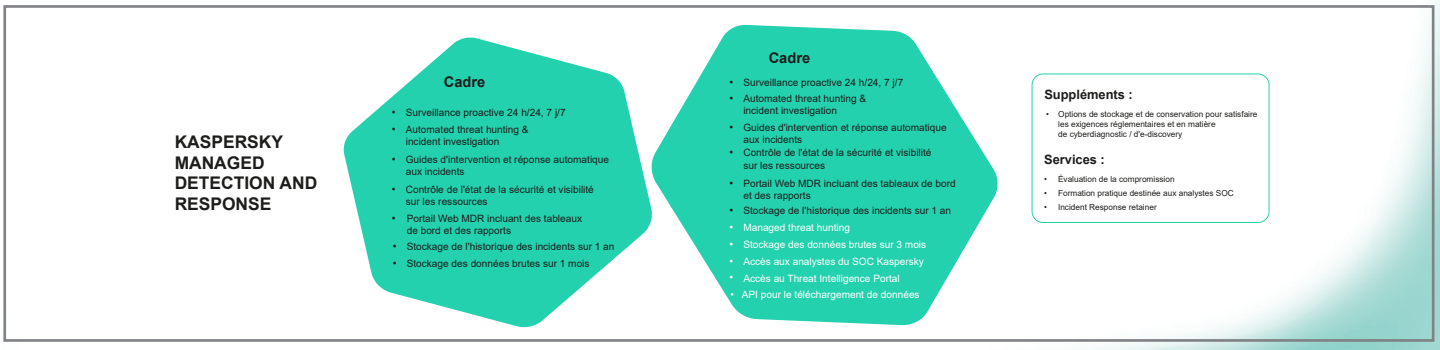
Produits pris en charge :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac*
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

Comment ça fonctionne ?

Kaspersky MDR valide les alertes produit pour garantir l'efficacité de la prévention automatique et analyse de manière proactive les métadonnées d'activité des systèmes, à la recherche du moindre signe d'une attaque active ou imminente. Ces métadonnées sont collectées via Kaspersky Security Network et sont automatiquement mises en corrélation en temps réel avec la Threat Intelligence inégalée de Kaspersky, afin d'identifier les stratégies, les techniques et les procédures utilisées par les attaquants. Les indicateurs d'attaque propriétaires permettent la détection des menaces furtives non malveillantes qui imitent des activités autorisées. Le produit s'adapte à votre infrastructure durant les deux à quatre premières semaines afin de garantir un taux de faux positifs nul, en vous demandant la confirmation de ce qui est légitime ou non.

Kaspersky MDR est disponible en deux versions, pour répondre aux besoins des organisations de toutes les tailles et des secteurs ayant des niveaux de maturité différents en matière de sécurité informatique (graphique 2). **Kaspersky MDR Optimum** accroît instantanément vos capacités de sécurité informatique sans avoir à investir dans du personnel ou des compétences supplémentaires. Cette solution renforce également votre résilience face aux attaques évasives, grâce à son déploiement clé en main rapide. **Kaspersky MDR Expert** inclut toutes les fonctionnalités de la version Optimum et fournit des fonctionnalités et une flexibilité étendues pour les équipes de sécurité informatique expérimentées. Cela leur permet de décharger les processus de triage et d'enquête des incidents sur Kaspersky et de consacrer leurs ressources internes limitées à la gestion des résultats critiques obtenus



Graphique 2. Versions de Kaspersky MDR

La recherche de menaces automatisée incluse dans la solution MDR Optimum utilise des détections automatiques s'appuyant sur des indicateurs d'attaque propriétaires à des fins de validation, d'investigation et d'identification plus poussées des nouvelles menaces. La recherche de menaces gérée offerte par la solution MDR Expert repose sur l'intervention manuelle fastidieuse de nos chercheurs de menaces expérimentés, qui traquent de manière proactive les menaces qui échappent à la détection automatique.

Un ensemble d'éléments complémentaires en option adapte les fonctionnalités du produit en fonction de vos besoins spécifiques, afin d'offrir une flexibilité accrue lorsque cela est nécessaire :

- Options de stockage et de conservation pour satisfaire les exigences réglementaires et en matière de cyberdiagnostic / d'e-discovery
- Un 'incident Response retainer' apporte toute l'expertise de Kaspersky pour résoudre vos incidents de sécurité
- Évaluation globale de la compromission pour vérifier que vos contrôles de sécurité existants sont suffisants
- Formation pratique destinée aux analystes SOC, afin d'assurer une préparation complète pour faire face aux incidents

Contrer les attaques ciblées requiert une expérience approfondie et un apprentissage constant. Kaspersky a été le premier éditeur de solutions de sécurité à créer, il y a près d'une dizaine d'années, un centre dédié à la recherche sur les menaces complexes, ce qui lui a permis de détecter plus d'attaques ciblées sophistiquées que tous ses concurrents. S'appuyant sur cette expertise unique, la solution Kaspersky Managed Detection and Response maximise la valeur de vos solutions de sécurité Kaspersky, en offrant des fonctionnalités entièrement gérées et personnalisées de détection, de hiérarchisation, d'enquête et de réponse en continu. Vous bénéficiez ainsi des principaux avantages d'un centre de sécurité sans même devoir en créer un.

* La prise en charge de Kaspersky Endpoint Security for Mac est prévue pour le premier trimestre 2021. Kaspersky ne fait aucune déclaration et ne prend aucun engagement concernant des dates de déploiement anticipées. Celles-ci sont fournies à titre informatif uniquement. Kaspersky se réserve le droit de modifier la planification des produits à tout moment.

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

www.kaspersky.fr

Nous sommes reconnus. Nous sommes indépendants. Nous sommes transparents. 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.