kaspersky 25 years

Kaspersky Optimum Security

Gardez une longueur d'avance sur les menaces évasives grâce à une solution complète EDR[1]/MDR[2] qui ne drainera pas vos ressources.

Kaspersky Optimum Security

30 % des cyberattaques réussies impliquent des outils système légitimes

Rapport analytique de Kaspersky concernant les réponses aux incidents, 2020

Le défi

Les ransomwares, les programmes malveillants et les logiciels espions financiers font preuve de plus en plus d'efficacité quand il s'agit d'échapper à la détection, et on peut également les acheter facilement sur le Dark Web à un tarif très abordable : la bête noire de nombreuses organisations aujourd'hui.

Le nombre d'attaques avancées est en hausse

Les menaces évasives d'aujourd'hui sont conçues pour contourner efficacement la protection traditionnelle des terminaux, ce qui engendre de nouveaux risques importants pour toutes les entreprises. Si une menace non détectée se propage dans votre infrastructure, vous pourriez subir des pertes importantes, ce qui aurait une incidence sur les résultats de l'entreprise :

- Interruption des processus métier stratégiques et perte de données
- atteinte importante à la réputation et perte de clients
- amendes, pénalités et pertes de profits

La protection des terminaux doit être renforcée

Les attaques les plus récentes **évitent la détection** en se dissimulant à l'intérieur d'outils système légitimes et à l'aide d'autres méthodes et technologies facilement accessibles : elles s'en servent pour **accéder au cœur de votre infrastructure et y réaliser des actions malveillantes et persistantes, tout ça en quelques instants et sans être détectées**.

Il y a ensuite le travail à distance, qui met les terminaux (c'est-à-dire habituellement la porte d'entrée la plus attrayante dans votre infrastructure), encore plus sous les projecteurs.

Et les ressources sont déjà très sollicitées

Pour fournir l'avantage supplémentaire dont vous avez besoin dès maintenant, votre organisation doit développer des capacités de réponse aux incidents adéquates.

Mais un projet comme celui-ci peut coûter très cher :

- les coûts des logiciels et du matériel peuvent s'additionner
- le cloisonnement et la fragmentation des outils et des processus entraînent une perte d'efficacité sur le plan de la sécurité
- les tâches de routine peuvent faire perdre du temps.

45 % des attaques ont été détectées en raison de fichiers suspects ou d'une activité suspecte sur les terminaux ; leur détection devient donc une priorité

Comme ci-dessus

Solution

Kaspersky Optimum Security offre une solution efficace de détection et de réponse aux menaces, soutenue par une surveillance de la sécurité 24h/24, 7j/7, des réponses automatisées et une recherche des menaces, ainsi que par le soutien et les conseils des experts de Kaspersky.

Protection optimale

Les méthodes de prévention automatique constituent le fondement de toute protection des terminaux, mais elles doivent être complétées par des outils avancés si vous vous retrouvez à devoir gérer les menaces évasives les plus dangereuses.

Kaspersky Optimum Security fournit offre des capacités avancées de détection basée sur le **Machine Learning** et de réponse rapide, le tout fourni depuis le cloud. Votre équipe peut désormais traiter avec rapidité et précision les menaces qui auparavant l'empêchaient de dormir la nuit.

Investissement optimal

Plus besoin d'embaucher plus de personnel, de former à nouveau vos employés ou de se prendre la tête avec des déploiements compliqués : Kaspersky Optimum Security simplifie les processus essentiels de réponse aux incidents et permet de les automatiser en fonction de vos besoins particuliers.

Nos options sur site et dans le cloud, associés à un ensemble d'outils de sécurité clés en main évolutifs, s'adaptent à vos besoins : vous pouvez ainsi simplifier votre système informatique, augmenter la productivité des utilisateurs et rendre les coûts de mise en œuvre transparents.

Équilibre optimal

Atteignez un équilibre optimal entre simplification et efficacité, intelligence humaine et automatisation, efficacité et fonctionnalité, sans pour autant compromettre votre protection !

Kaspersky Optimum Security vous permet de réduire les risques liés à la perte d'argent, de clients et de réputation, et renforce vos défenses contre les nouvelles menaces inconnues et évasives. Vous êtes donc prêt à faire face à l'évolution rapide du contexte actuel des menaces.

Principaux avantages

- **Défendez votre entreprise contre le risque réel de dommages et de perturbations** liés à la dernière vague de menaces évasives dangereuses.
- **Mettez au point votre propre système de réponse aux incidents** grâce à un ensemble d'outils EDR (Endpoint Detection and Response) simple à utiliser.
- **Renforcez facilement vos capacités de détection** grâce à une solution MDR (Managed Detection and Response) puissante et très simple à utiliser.
- Réduisez considérablement vos risques d'être infecté **en formant vos employés et en les sensibilisant à la sécurité.**
- Conservez des ressources précieuses grâce à **l'automatisation des opérations et à la gestion de la protection.**
- Gagnez du temps et réduisez vos efforts grâce à une solution dont les diverses fonctionnalités sont toutes gérées **dans un seul service cloud ou une seule console sur site**

55 % des attaques ont mis plusieurs semaines, voire beaucoup pour être détectées

Comme ci-dessus

Principales fonctionnalités

Kaspersky Optimum Security offre un large éventail de fonctionnalités essentielles pour la protection contre les menaces évasives, au cœur desquelles se trouvent la détection, l'analyse et la réponse.

Détection avancée

- **Algorithmes d'analyse du comportement fondés sur le** Machine Learning permettant de détecter rapidement et précisément les comportements suspects.
- **Recherche automatisée de menaces** fondée sur des indicateurs d'attaque (IoA) exclusifs permettant de découvrir toutes les menaces complexes cachées, avec l'aide des experts Kaspersky.
- Contrôle évolutif des anomalies permettant **d'adapter automatiquement la configuration des outils de réduction de la surface d'attaque** en fonction du profil utilisateurs.
- Détection cloud et **sandboxing intégré dans le cloud**.

Analyse simple

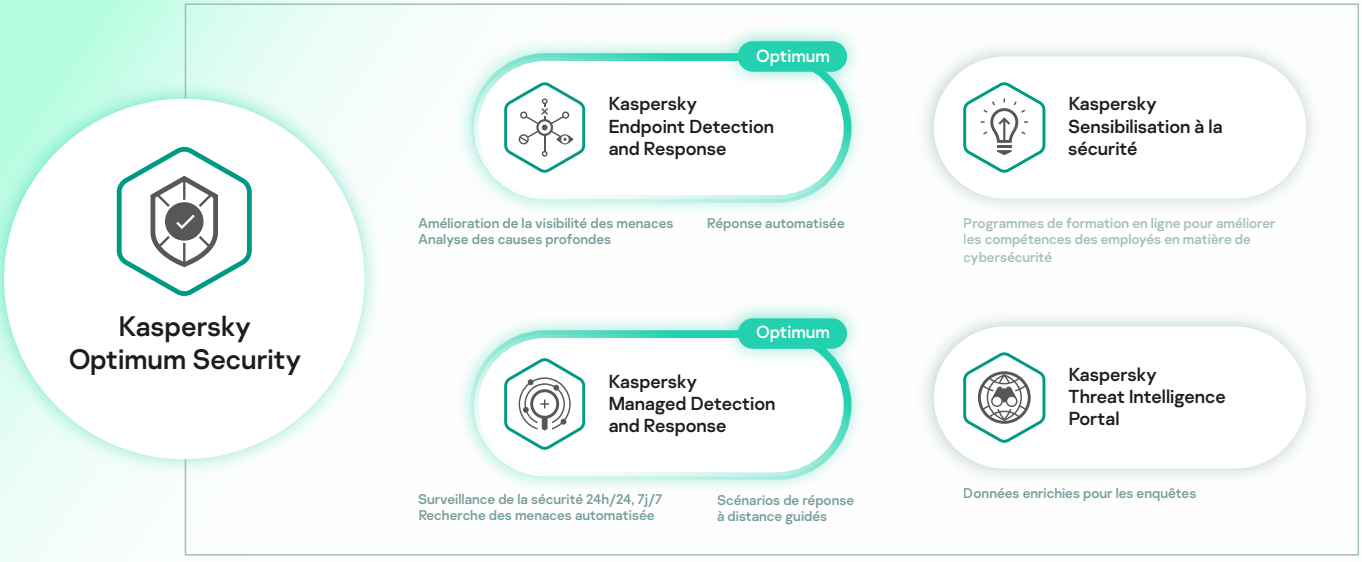
- Toutes les informations relatives à un incident sont automatiquement rassemblées dans **une carte d'incident unique**.
- **La visualisation et un processus d'enquête simple** vous permettent d'analyser rapidement et efficacement l'incident dans un environnement unique, puis de décider de la suite des opérations.
- En même temps, toutes les détections effectuées par les indicateurs d'attaque sont **classées par ordre de priorité et examinées par Kaspersky pour vous fournir des recommandations sur mesure**.

Réponse automatisée

- **Une réponse « en un seul clic »** vous permet de contenir rapidement tout incident isolé.
- **Une réponse guidée** reposant sur l'expérience de nos experts vous permet de faire face aux menaces les plus complexes et les plus dangereuses.
- **La réponse croisée automatisée sur plusieurs terminaux** vous permet de trouver les menaces analysées ou importées sur le réseau et d'y répondre.

Sommaire

Choisissez la façon dont vous souhaitez utiliser Kaspersky Optimum Security : comme solution managée pour assurer une protection 24h/24, 7j/7 ; comme un ensemble d'outils EDR facile à utiliser ; ou comme un mélange des deux, en profitant de l'expérience et des connaissances des experts de Kaspersky tout en développant vos capacités de détection et de réponse en interne. Kasperky Optimum Security réunit plusieurs produits dans une seule solution :



Les emails malveillants ont été à l'origine de 31 % des cyberattaques réussies, ce qui signifie que beaucoup d'entre elles auraient pu être évitées par les employés eux-mêmes

Comme ci-dessus

Mais attendez, ce n'est pas tout...

Renforcez davantage vos défenses grâce à des outils destinés à différents aspects de votre sécurité : détection, enquête et sensibilisation.

Formez vos utilisateurs

La clé pour réduire votre surface d'attaque ainsi que le nombre d'incidents est de former vos employés afin qu'ils soient conscients des cyber-menaces qu'ils peuvent diffuser sur votre infrastructure par négligence ou par simple manque de connaissances. **Kaspersky Security Awareness** permet de développer les connaissances et les compétences dont tous les employés ont besoin pour protéger votre infrastructure. Ainsi, votre personnel travaille activement avec vous pour maintenir un environnement sécurisé.

Hachage

Profitez des informations les plus récentes

Aidez vos spécialistes de la cybersécurité à analyser et à approfondir leur compréhension des menaces grâce aux dernières informations concernant les fichiers, les hachages, les adresses IP et les URL associés aux menaces. Profitez de cet aperçu supplémentaire sans coût additionnel grâce au **Kaspersky Threat Intelligence Portal**, facile à utiliser.

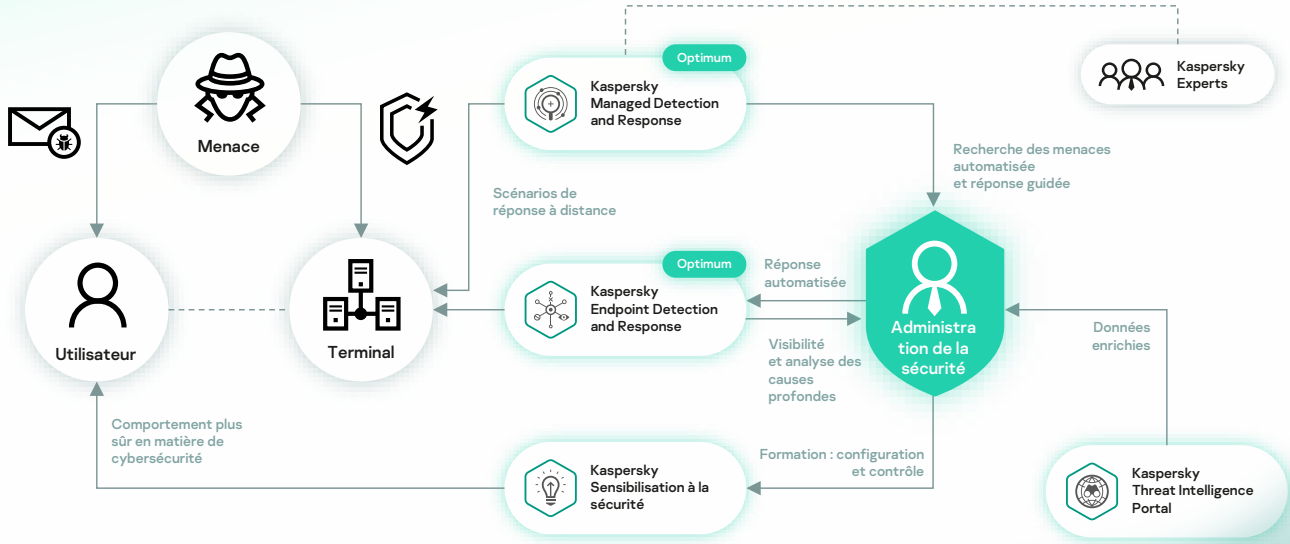
Laissez-nous vous aider

Pour assurer la bonne protection de votre infrastructure informatique, vous devez implémenter et configurer vos produits en vous référant aux bonnes pratiques et à vos exigences en matière de sécurité.

Maximisez le retour sur investissement de votre solution de sécurité et assurez-vous qu'elle fonctionne à 100 % en laissant nos experts des **services professionnels Kaspersky** vous aider à vérifier, mettre en œuvre, mettre à jour et optimiser votre solution de sécurité.

Fonctionnement de l'ensemble de la solution

La prévention, la détection, l'analyse, la réponse et la formation des employés sont réunies dans Kaspersky Optimum Security. Chaque composant a une fonction définie et peut être utilisé de manière indépendante, mais c'est en fonctionnant ensemble qu'ils couvrent tous vos besoins de protection évasive des terminaux sous la forme d'une solution intégrée unique.



44 % des entreprises considèrent le coût de la sécurisation d'environnements de plus en plus complexes comme l'un des principaux problèmes

Rapport « IT security economics 2021 » (Économie de la sécurité informatique 2021)

Fonctionnement simple

Kaspersky Optimum Security est facile à gérer à partir d'une console unique, ce qui vous permet de rentabiliser au maximum votre temps et vos ressources limités.

Offre complète

- Cette offre fait partie de l'écosystème de sécurité de Kaspersky qui vous permet de renforcer vos défenses, qu'il s'agisse des bases de la sécurité ou des fonctionnalités avancées optimisées.
- Les diverses fonctionnalités de Kaspersky Optimum Security peuvent être gérées depuis une console unique dans le cloud.
- Plusieurs couches de protection traitent à la fois les menaces basiques et les menaces évasives, ainsi que les risques d'erreur humaine.

Administration simplifiée

- La console de gestion dans le cloud vous offre un outil de gestion rapide et efficace à utiliser depuis partir de n'importe quel endroit du monde.
- Les solutions sur site et SaaS offrent la même expérience d'administration.
- Le déploiement est rapide et sans tracas, que vous utilisiez déjà ou non les solutions Kaspersky.
- Votre équipe peut contrôler et gérer facilement et intuitivement tous les outils, sans besoin de longue prise en main ni de nouvelle formation.

Gain de temps et de ressources

- La protection managée vous permet de développer des capacités de détection et de réponse sans les investissements de sécurité associés, même si vous manquez de personnel ou d'expertise en matière de cybersécurité.
- Les processus essentiels sont automatisés, ce qui rend la réponse aux incidents rapide, précise et efficace.
- Une meilleure sensibilisation des employés à la sécurité se traduit par une diminution des menaces qui franchissent vos défenses et donc par une réduction du nombre d'incidents à traiter !

Dans la pratique

Comment tout s'articule concrètement.

Infiltration

L'utilisateur reçoit un email de phishing ou accède à une ressource Internet malveillante, infectant son hôte

- Sensibilisation des employés à la sécurité
- Réduction de la surface d'attaque
- Prévention automatique des menaces

Installation

L'infection initiale déploie les composants nécessaires, communique avec C&C[1] et explore son environnement

- Mécanismes de détection avancés, notamment l'analyse comportementale basée sur le Machine Learning et le sandboxing dans le cloud
- Recherche des menaces automatisée avec IoA (indicateurs d'attaque)[2]
- Analyse des causes profondes et analyse des IoC (indicateurs de compromission)[3]
- Scénarios de réponse à distance guidés

Accès racine

Une série d'outils est utilisée pour gagner en persistance et amorcer un mouvement horizontal si nécessaire

[1] Commandement et contrôle
[2] Indicateurs d'attaque
[3] Indicateur de compromission

Approche par étape de Kaspersky

Ensemble, nous pouvons construire vos défenses en nous appuyant sur une protection fiable avec Kaspersky Security Foundations, en évoluant en douceur vers une réponse aux incidents essentiels avec Kaspersky Optimum Security, et finalement en passant à des outils puissants qui assurent une protection contre les menaces les plus avancées, avec Kaspersky Expert Security. Choisissez la solution la mieux adaptée à vos besoins :

Kaspersky Security Foundations

Bloquez automatiquement la grande majorité des menaces.

» En savoir plus

Kaspersky Optimum Security

Renforcez vos défenses contre les menaces évasives.

» En savoir plus

Kaspersky Expert Security

Assurez une protection contre les attaques complexes et de type APT.

» En savoir plus

À propos de nous

Nous sommes une entreprise privée mondiale de cybersécurité qui compte des centaines de milliers de clients et de partenaires dans le monde entier, engagée envers la transparence et l'indépendance. Depuis 25 ans, nous développons des outils et fournissons des services visant à assurer votre sécurité grâce à nos technologies les plus testées et les plus primées.

IDC

Rapport IDC MarketScape sur l'évaluation des fournisseurs, catégorie « Worldwide Modern Endpoint Security for Enterprises 2021 »

Acteur principal

Tests AV

Protection avancée pour les terminaux : test de protection contre les ransomwares

Protection totale

Radicati Group

Market Quadrant sur les menaces persistantes avancées (APT)

Acteur principal

Étudiez tout cela de plus près

Pour en savoir plus sur la manière dont Kaspersky EDR Optimum traite les cyber-menaces tout allégeant la charge de travail de votre équipe de sécurité et vos ressources, rendez-vous sur le site www.kaspersky.fr/enterprise-security/edr-security-software-solution

[1]Endpoint Detection and Response
[2]Managed Detection and Response

Actualités des cybermenaces : viruslist.com/fr
Actualités dédiées à la sécurité informatique : kaspersky.fr/business
Sécurité informatique pour les PME : kaspersky.fr/business
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

kaspersky.fr