Kaspersky Endpoint Detection and Response Optimum

Faites passer votre protectio des terminaux à la vitesse supérieure et affrontez les menaces évasives en toute tranquillité.

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

Il est temps de passer à la vitesse supérieure. Vous êtes prêt non seulement à protéger votre organisation avec des technologies essentielles 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.

Les défis

Menaces échappant à la détection

Les programmes malveillants évasifs, les ransomwares, les logiciels espions et autres menaces font preuve d'une sophistication pour éviter les mécanismes de détection traditionnels, en utilisant des outils système légitimes et d'autres techniques avancées pour leurs attaques.

64 % des organisations ont déjà été victimes d'attaques de ransomwares. Parmi elles, 79 % ont payé la rançon à leurs attaquants.

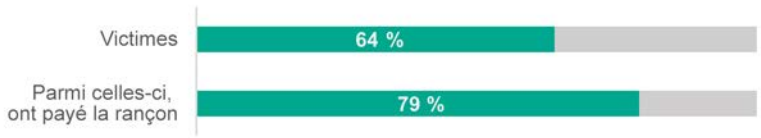
Kaspersky, mai 2021

Ransomware en tant que service

Les pirates peuvent acheter des outils prêts à l'emploi à bas prix et attaquer n'importe qui, en volant des données, en endommageant votre infrastructure et en exigeant des rançons toujours plus élevées.

Des ressources limitées

Les infrastructures deviennent de plus en plus complexes et étendues, tandis que les ressources (le temps, l'argent et la durée d'attention) sont insuffisantes. Il n'y a plus de place pour le superflu.



« Les solutions complètes, la fiabilité et la rapidité du service et de l'assistance de Kaspersky sont importantes pour nous. Ils garantissent la disponibilité de notre environnement informatique. »

Marcelo Mendes, RSSI, NEO
lire l'étude de cas

Nos solutions pour y faire face

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.

Protection avancée

Nos mécanismes de détection avancés intègrent diverses technologies telles que le Machine Learning, l'analyse comportementale et le sandboxing dans le cloud.

Des outils d'analyse visuelle simples vous permettent de comprendre pleinement la menace et son champ d'application ; et des actions de réponse rapides bloquent l'attaque en cours, avant tout dommage.

Une solution unique

La sécurité des terminaux de nouvelle génération vous est proposé dans une solution EDR simple à utiliser pour une protection renforcée des ordinateurs portables, des postes de travail, des serveurs, des charges de travail cloud et des environnements virtuels.

Tout ce déploiement et cette gestion se déroulent au même endroit sous la forme d'une console unique, dans le cloud ou sur site.

Simple et efficace

Nous avons conçu EDR Optimum en pensant aux petites équipes de cybersécurité, qui cherchent à moderniser leurs fonctionnalités de réponse aux incidents et à développer leur expertise, mais n'ont pas beaucoup de temps disponible.

Nous automatisons et optimisons la plupart des tâches, afin que vous ayez plus de temps à consacrer à ce qui est vraiment important.

Principaux avantages

- **Bloquez plusieurs types** de menaces
- **Protégez vos systèmes et vos données contre** les menaces évasives
- **Détectez les menaces actuelles** avant qu'elles n'agissent
- **Identifiez les menaces évasives** sur l'ensemble de vos terminaux
- **Comprenez les menaces** et analysez-les rapidement
- **Prévenez les dommages** grâce à une réponse automatisée rapide
- **Gagnez du temps et des ressources** grâce à un seul outil simplifié
- **Défendez chaque terminal :** ordinateurs portables, serveurs, charges de travail dans le cloud

Principales fonctionnalités

- Sécurité **inhérente des terminaux nouvelle génération**
- **Détection avancée** basée sur le Machine Learning
- **Balayage des indicateurs** de compromission (IoC)
- **Outils** visuels d'investigation et d'analyse
- Toutes les données nécessaires dans une **seule carte d'alerte**
- **Guidage et automatisation** intégrés des réponses
- **Automatisation et console Cloud unique** ou sur site
- Prend en charge les **postes de travail, les serveurs virtuels et physiques, les déploiements VDI (infrastructures de bureaux virtuels) et les charges de travail du cloud public**

Principaux cas d'utilisation

Suis-je victime d'une attaque ?

- **La détection avancée**, basée sur le Machine Learning et intégrant le sandboxing dans le cloud, décèle automatiquement les menaces.
- **Téléchargez et analysez les IoC** à partir de securelist.com ou d'autres sources pour détecter les menaces avancées.

Puis-je la neutraliser ?

- **Utilisez plusieurs options de réponse :** isolez l'hôte, empêchez l'exécution du fichier ou supprimez-le.
- **Scannez les autres hôtes** afin de détecter les signes de la menace analysée.
- **Appliquez une réponse automatique** sur tous les hôtes lors de la découverte d'une menace (IoC).

Comment développer mes compétences ?

- **Consultez les recommandations de réponse** dans la carte d'alerte.
- **Accédez auportail Threat Intelligence** et aux dernières informations en matière de surveillance des menaces.
- **Développez votre expertise** par l'analyse et la réponse aux menaces.

Comment cela a-t-il pu arriver ?

- Analysez la menace sous forme d'**arborescence virtuelle des processus.**
- Suivez ses actions sur un **graphique détaillé.**
- **Cernez sa cause profonde et son point d'entrée** dans les infrastructures.

Comment faire pour que cela ne se reproduise pas ?

- **Exploitez les informations apprises :** connaître les adresses IP et sites Web à bloquer, les politiques à modifier et les employés à former.
- **Créez des règles visant à bloquer** ces menaces à l'avenir, comme empêcher l'exécution du fichier.

Qu'en est-il des menaces dites « basiques » ?

- **La sécurité des terminaux de nouvelle génération** est intégrée afin de stopper immédiatement la plupart des menaces.
- **Améliorez vos correctifs grâce à la** gestion des vulnérabilités et des correctifs.
- **Automatisez la réduction de votre surface d'attaque** et l'adaptation des politiques grâce aux contrôles des terminaux.

Comment ça fonctionne ?

Pour une démonstration rapide, consultez cette vidéo.

D'où venez-vous ?

Vous disposez d'une protection contre les programmes malveillants, mais ce n'est pas suffisant ?

Renforcez la protection de vos terminaux

Que vous utilisiez Kaspersky ou une protection tierce pour vos terminaux, c'est le bon moment de réfléchir à la mise en œuvre de l'EDR.

Il n'est pas seulement question d'améliorer les capacités de détection et de prévention, mais également de se préparer face aux menaces évasives, en les identifiant, en les analysant et en les neutralisant.

Apprenez-en davantage sur la protection contre les menaces évasives grâce au **Guide d'achat pour une sécurité optimale**.

Vous utilisez déjà Kaspersky ?

Optimisez votre sécurité

Nous améliorons en continu nos produits, alors assurez-vous d'utiliser pleinement nos solutions en adoptant une version supérieure ; ou bien passez au cloud et oubliez totalement les tâches de routine ennuyeuses.

La dernière version de Kaspersky EDR Optimum offre les fonctionnalités suivantes :

- Réponse guidée dans les cartes d'alerte !
- Vérification des objets critiques du système avant application de la réponse !
- Réputation du fichier indiquée dans les cartes d'alerte grâce à la surveillance des menaces !
- Profondeur illimitée d'analyse de l'arborescence des processus !

Découvrez les nouvelles fonctionnalités en détail **ici**.

Vous découvrez Kaspersky Lab ?

Optimisez votre sécurité

Des milliers d'entreprises dans le monde utilisent Kaspersky EDR Optimum pour les avantages suivants :

- Solution EPP puissante et EDR de base dans le même produit
- Fonctionnalités EDR simples à utiliser conçues pour les petites équipes de cybersécurité
- Une solution légère et flexible avec déploiement dans le cloud ou sur site

Découvrez **Kaspersky Optimum Security**, une solution complète contre les menaces évasives, reposant sur les technologies EDR et MDR

Lancez-vous selon une approche progressive

Les outils que vous utilisez doivent être parfaitement adaptés à vos besoins en matière de cybersécurité et à ceux de votre entreprise, ainsi qu'à votre équipe et à vos ressources. Nous avons donc simplifié le choix du niveau de cybersécurité sur lequel vous vous concentrez actuellement, avec trois options différentes en fonction du profil de votre organisation.

Kaspersky Security Foundations

Bloquez automatiquement la grande majorité des menaces.

- La prévention automatisée multi-vecteurs des incidents causés par des menaces primaires : la grande majorité des cyberattaques.
- La première étape 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.

» En savoir plus

Kaspersky Optimum Security

Renforcez vos défenses contre les menaces évasives. Cette solution est adaptée à votre entreprise si :

- Elle dispose d'une petite équipe de sécurité informatique ayant une expertise de base en matière de cybersécurité.
- Elle dispose d'un environnement informatique dont la taille et la complexité évoluent, ce qui élargit la surface d'attaque.
- Elle manque de ressources en matière de cybersécurité tout en ayant besoin d'une protection renforcée.
- Elle a un besoin croissant de développer une capacité de réponse aux incidents.

» En savoir plus

Kaspersky Expert Security

Assurez une protection contre les attaques complexes et de type APT. Cette solution est adaptée aux entreprises ayant :

- Des environnements informatiques complexes et distribués.
- Une équipe de sécurité informatique mature ou un centre d'opérations de sécurité (SOC) établi.
- Une aversion pour le risque en raison des coûts plus élevés des incidents de sécurité et des violations de données.
- Des activités dans un domaine au sein duquel on se préoccupe de respect des réglementations.

» 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

Et si vous avez besoin d'encore plus

Découvrez Kaspersky EDR Expert, un puissant outil EDR pour offrir à vos experts des fonctionnalités approfondies de chasse aux menaces, une personnalisation détaillée et des mécanismes de détection supérieurs.

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

---

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

kaspersky.fr