Kaspersky® Endpoint Security

La principale plateforme de protection multiniveaux pour tous les terminaux, reposant sur de véritables technologies de cybersécurité

L'environnement des menaces évolue de manière exponentielle, si bien que les processus stratégiques, les données confidentielles et les ressources financières sont de plus en plus menacés par des attaques « zero-day ». Au cours des 12 derniers mois, plus de 38 % de l'ensemble des entreprises ont été touchés par une forme de programme malveillant. Pour atténuer les risques au sein de votre entreprise, vous devez être plus intelligent, mieux équipé et mieux informé que les cybercriminels.

La majorité des cyberattaques qui touchent les entreprises est lancée via le terminal. Si vous pouvez sécuriser de manière efficace chaque terminal de l'entreprise, qu'il soit physique ou virtuel, statique ou mobile, vous disposez alors d'une base solide pour votre stratégie globale en matière de sécurité.

Les technologies et la Threat Intelligence de Kaspersky Lab évoluent en permanence pour protéger votre activité contre les menaces et les failles les plus récentes et les plus poussées, y compris contre les attaques ciblées.

Cette protection instantanée contre les menaces connues et inconnues est renforcée par de puissants outils de contrôle et de protection des données, dont le chiffrement intégré, l'application automatique de correctifs et la protection des terminaux mobiles, tous administrés via une seule console, Kaspersky Security Center.

Prévention des menaces

Notre moteur de prévention des menaces, exploitant la veille stratégique HuMachine™, vous protège contre les ransomwares, l'exploitation des failles et même les cybermenaces les plus sophistiquées.

Contrôle des terminaux avancé

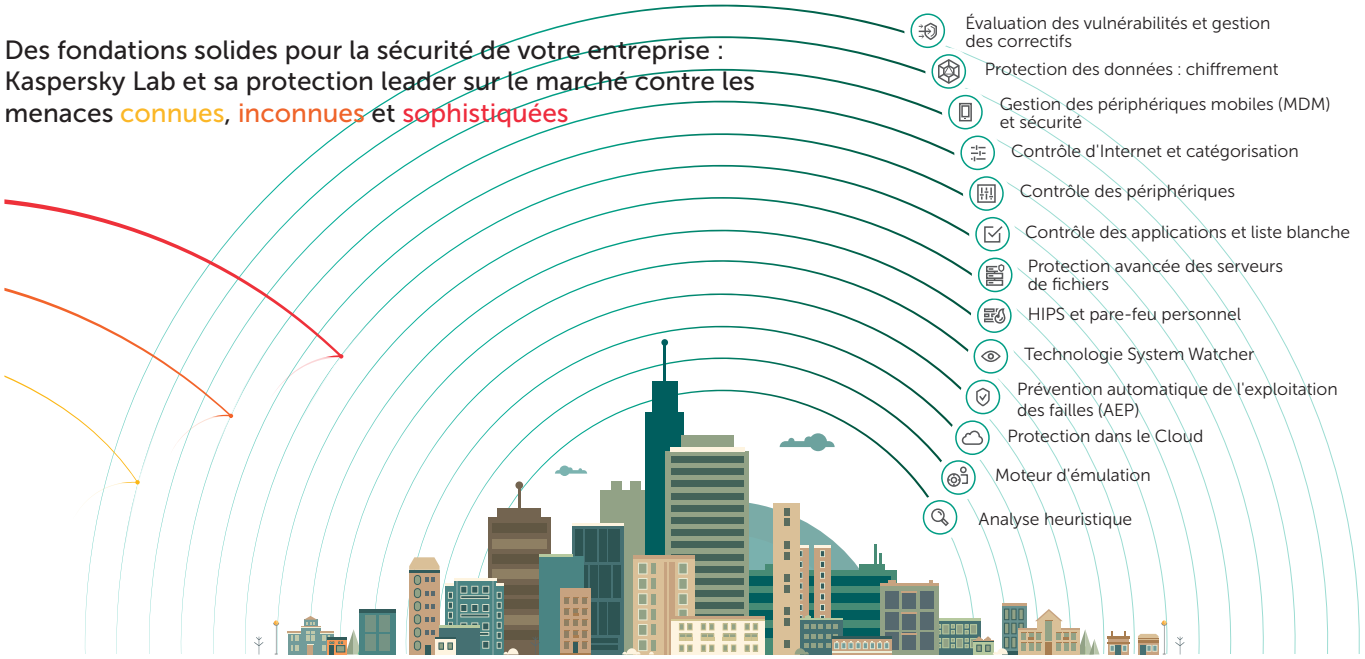
Des contrôles centralisés simples et efficaces des applications, des appareils et du Web réduisent votre surface d'attaque et permettent d'assurer la sécurité des utilisateurs.

Protection des données

La technologie de chiffrement intégral de disque certifiée FIPS 140.2 facilite la protection complète des données confidentielles sur les appareils fixes et mobiles.

Protection multiniveaux

Des fondations solides pour la sécurité de votre entreprise : Kaspersky Lab et sa protection leader sur le marché contre les menaces connues, inconnues et sophistiquées



PUISSANTE PROTECTION MULTINIVEAUX CONTRE TOUTES LES FORMES DE CYBERMENACES

Sécurité sans précédent grâce au machine learning

La sécurisation totale de chaque terminal contre toute forme de cybermenace connue et inconnue est une mission essentielle. La protection traditionnelle contre les programmes malveillants n'est en aucun cas suffisante. Ce n'est qu'en employant une plateforme de sécurité de pointe et en adoptant une approche multiniveaux que vous pouvez espérer protéger totalement chaque terminal, dans et au-delà de votre périmètre.

Haute performance

La sécurité intégrée unique de Kaspersky Lab bat en continu au cœur de votre infrastructure informatique, appliquant une protection puissante via un agent de terminal unique avec des répercussions minimes sur la vitesse ou les ressources. Développée en interne en tant que plateforme intégrée, entièrement évolutive, la solution permet de bénéficier de performances optimales, sans conflit avec les logiciels ni faille de sécurité.

Puissante surveillance des menaces

C'est en se fondant sur des sources inégalées de surveillance en temps réel des menaces que nos technologies évoluent continuellement pour protéger votre entreprise, même des menaces les plus sophistiquées et les plus récentes, y compris les menaces « zero-day ». En alignant votre stratégie de sécurité aux leaders mondiaux de la détection des menaces avancées, vous vous dotez de la meilleure protection des terminaux d'aujourd'hui et de demain. Il n'existe pas de meilleur choix en matière de sécurité pour votre entreprise.

Gestion unifiée et centralisée

Gérez plusieurs plateformes et appareils depuis la même console utilisée pour vos autres terminaux et gagnez en visibilité et en contrôle, sans effort ou technologie d'administration supplémentaires.

Élimination et prévention inégalées des menaces de nouvelle génération

Au cœur de notre stratégie de sécurité figure le moteur de protection des terminaux le plus puissant et le plus efficace du secteur (comme le confirment en permanence des tests indépendants[1]) alimenté par une veille stratégique et des technologies de machine learning performantes.

Les niveaux de protection intelligente et proactive se superposent pour constituer des défenses puissantes et solides contre les cybermenaces avancées, connues et inconnues les plus sophistiquées.

- Analyse heuristique **et émulation de menaces basées sur plusieurs algorithmes** : détecte les programmes malveillants inconnus **et complète les technologies** traditionnelles basées sur les signatures.
- **Protection assistée par le Cloud Kaspersky Security Network (KSN)** : facilite l'identification et le blocage des nouveaux programmes malveillants dès leur apparition.
- **Prévention automatique de l'exploitation des failles** : permet d'arrêter de manière proactive les menaces les plus avancées en bloquant les failles utilisées par les cybercriminels.
- **Surveillance du système** : bloque les menaces inconnues en détectant les comportements suspects et rétablit les fichiers clés si le système a été touché ; protection fiable contre les ransomwares.
- **Système de prévention des intrusions basé sur l'hébergeur (HIPS)** : limite les activités et accorde les droits d'accès en fonction du niveau de fiabilité du logiciel.
- **Le pare-feu personnel** limite l'activité du réseau.
- **La prévention des intrusions** stoppe les attaques réseau.

[1] www.kaspersky.fr/top3

Protection contre les ransomwares et l'exploitation des failles

Protégez vos données et évitez de financer les cybercriminels en payant les rançons grâce à Kaspersky System Watcher. Protégez les dossiers partagés contre les cryptoverrouilleurs avancés à l'aide de Kaspersky Security for Windows Server. Et protégez l'ensemble de vos terminaux contre les vulnérabilités les plus récentes à l'aide de nos technologies de prévention automatique d'exploitation des failles.

Réduisez votre exposition aux attaques via les applications

Fonctionnant avec **la création dynamique de listes blanches, le contrôle des applications** réduit drastiquement votre exposition aux attaques « zero-day » en vous fournissant un contrôle total sur le logiciel autorisé à s'exécuter. Les applications figurant sur la liste noire sont bloquées, tandis que celles dont le comportement est suspect ou inapproprié sont détectées, analysées puis bloquées ou limitées à l'aide de System Watcher ou de l'HIPS. Dans le même temps, les applications fiables que vous avez approuvées continuent de fonctionner avec fluidité.

Création de listes blanches flexibles dans le Cloud

La **création de listes blanches** par notre laboratoire interne prend en charge un scénario de **blocage par défaut**, qui peut être exécuté dans un environnement testé.

Parer les dangers de la navigation sur Internet

Le contrôle d'Internet surveille, filtre et contrôle chaque site Internet auquel les utilisateurs finaux peuvent accéder sur leur lieu de travail, ce qui permet d'augmenter la productivité tout en réduisant votre vulnérabilité à la pénétration et à l'infiltration des systèmes via les sites Internet et les réseaux sociaux.

Contrôle de l'utilisation des appareils portables

Le contrôle des appareils vous protège contre les conséquences dramatiques de la perte des données des clients ou de l'entreprise présentes sur des appareils portables non chiffrés ou non approuvés, ainsi que contre le téléchargement de données infectées à partir de l'appareil.

Application d'une protection avancée aux serveurs de l'entreprise

Le **Contrôle du lancement des applications** sur les serveurs offre une sécurité sans précédent, grâce à l'utilisation de règles configurées dans le but d'autoriser ou de bloquer le lancement de fichiers exécutables, de scripts et de paquets MSI ou le chargement de modules DLL sur les serveurs.

Contrôlez chaque terminal

Réduisez l'exposition au risque des terminaux tout en gagnant en productivité. Contrôlez l'accès de chaque terminal aux applications, sites Internet et appareils en identifiant et bloquant les terminaux inappropriés, en régulant l'accès des terminaux non nécessaires et en favorisant les terminaux utiles et fiables.

Tous les outils de contrôle s'intègrent à Active Directory ; la création et l'application des polices automatisées, personnalisables ou simplifiées peuvent être centralisées ou basées sur le rôle selon votre préférence.

Protection des données via un chiffrement intégré certifié FIPS 140-2

Le chiffrement puissant et transparent vis-à-vis des utilisateurs sécurise totalement les données sensibles et confidentielles sur les mobiles, les appareils portables et fixes. Cette technologie intégrée vous permet d'appliquer de manière centralisée le chiffrement des données de l'entreprise au niveau de l'appareil, du disque ou du fichier, par l'intermédiaire de politiques de sécurité applicables à des groupes de terminaux ou à un appareil en particulier. Le tout via la même console unique utilisée pour gérer l'ensemble de la sécurité Kaspersky Lab de vos terminaux, avec le chiffrement intégré du système d'exploitation, dont Microsoft BitLocker.

Supprimer les vulnérabilités grâce à l'application automatique des correctifs

L'exploitation des vulnérabilités découvertes dans une application fiable est l'une des méthodes les plus courantes d'accéder à l'infrastructure informatique par l'intermédiaire d'un seul terminal. La hiérarchisation et la gestion efficaces et opportunes des correctifs des vulnérabilités requièrent une profonde connaissance des failles, de leurs comportements et de leurs cibles réelles. Le système automatique de **gestion des correctifs et d'évaluation des vulnérabilités** de Kaspersky Lab repose sur des informations globales en temps réel à propos des activités d'exploitation des failles et permet de tenir à jour les correctifs essentiels, sans impacter les utilisateurs ou les systèmes occupés.

Sécuriser les appareils mobiles au-delà de votre périmètre

Les données de votre entreprise sont désormais accessibles partout et à tout moment sur les smartphones et les tablettes qui transitent librement dans votre périmètre informatique. **La sécurité mobile** vous protège contre les menaces qui ciblent les données sensibles des mobiles, et contre celles qui exploitent les failles de sécurité des appareils des salariés ou de l'entreprise pour infiltrer les systèmes.

Optimisation de l'efficacité : gestion intégrée

Kaspersky Endpoint Security permet à vos équipes en charge de la sécurité de bénéficier d'une visibilité intégrale et d'un contrôle total sur chaque poste de travail, serveur ou appareil mobile qui se trouve dans votre périmètre, où qu'il se trouve et quoi qu'il fasse. Pratiquement adaptable à l'infini, la solution permet d'accéder aux inventaires, aux licences, au dépannage à distance et aux contrôles du réseau à partir d'une console unique : le **Kaspersky Security Center**.

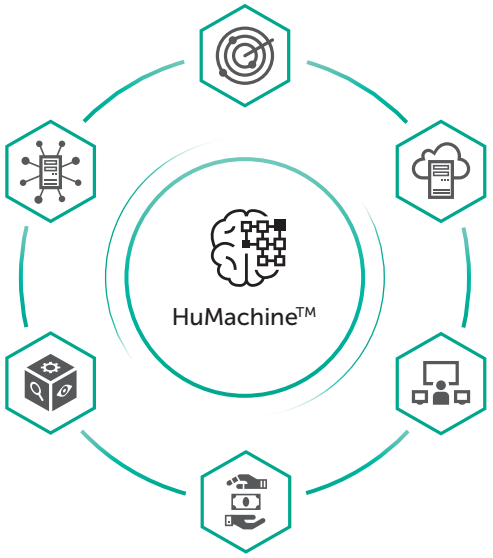
La gestion centralisée à partir d'une console unique est complétée par la fonction de gestion basée sur les rôles. De ce fait, les droits d'accès et les responsabilités peuvent être attribués à des professionnels de la sécurité différents selon les besoins.

Vision globale des solutions de sécurité pour les entreprise de Kaspersky Lab

Bien qu'elle soit essentielle, la protection des terminaux ne constitue que la première étape. Que vous exécutiez une stratégie de sécurité complexe ou à source unique, Kaspersky Lab propose **de nombreuses solutions pour les entreprises**, qui se combinent ou fonctionnent en parfaite indépendance afin que vous puissiez faire votre choix en toute liberté sans sacrifier l'efficacité et les performances. Nos solutions protègent les **systèmes virtuels et basés dans le Cloud** ainsi que les **terminaux, les serveurs et les infrastructures physiques**. Elles s'intéressent également à des questions de cybersécurité propres à des **secteurs d'activité spécifiques** comme les services financiers, les services de santé et les gouvernements.

Anti Targeted Attack

Identification exhaustive de plusieurs vecteurs, atténuation des risques de menaces avancées et d'attaques ciblées



Endpoint Security

La principale plateforme de protection multiniveaux pour tous les terminaux, reposant sur de véritables technologies de cybersécurité

Sécurité dans le Cloud

Une sécurité sans limite, spécialement conçue pour votre Cloud hybride

Services de cybersécurité

Exploitation de Threat Intelligence, formation à la sécurité, réponse aux incidents et évaluation des risques

Centre de supervision de la sécurité (SOC)

Équiper votre SOC d'outils et d'informations permettant de détecter efficacement les menaces et prendre des mesures correctives contre elles

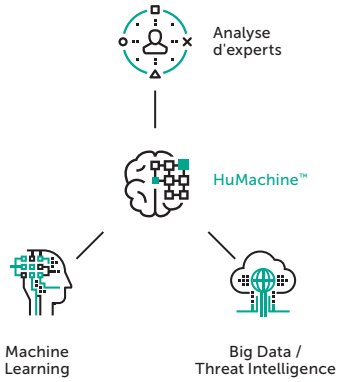
Fraud Prevention

Détection proactive des fraudes en temps réel, quels que soient les canaux

Maintenance et assistance

Opérant dans plus de 200 pays, à partir de 34 bureaux répartis dans le monde entier, notre engagement permanent d'assistance (24h/24, 7j/7, 365 jours par an) se reflète dans notre **Contrat de maintenance et d'entretien (MSA)**. Nos équipes en charge des **services professionnels** sont prêtes à intervenir à tout moment pour que vous puissiez profiter au maximum des avantages de votre installation de sécurité Kaspersky Lab.

Pour découvrir comment sécuriser plus efficacement vos terminaux, veuillez contacter l'équipe commerciale de Kaspersky Lab Enterprise.



Kaspersky Lab
pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr