KASPERSKY ENDPOINT SECURITY FOR ENTERPRISE

La solution nouvelle génération de protection contre les menaces avancées visant vos terminaux et vos utilisateurs

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 ». Pour atténuer les risques au sein de votre entreprise, vous devez être plus intelligent, mieux équipé et mieux informé que les cybercriminels.

Mais c'est une réalité : 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 statique ou mobile, vous disposez alors d'une base solide pour votre stratégie globale en matière de sécurité.

SÉCURITÉ PUISSANTE

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

PERFORMANCES PUISSANTES

La protection des terminaux doit sembler aussi naturelle et se faire de manière aussi inconsciente que la respiration. La plateforme de sécurité intégrée unique de Kaspersky Lab bat en continu au cœur de votre infrastructure informatique, appliquant une protection puissante aux terminaux avec des répercussions minimes sur la vitesse ou les ressources. Développée en interne en tant que plateforme intégrée, entièrement évolutive et unique, la solution permet de bénéficier de performances optimales sans conflit avec les logiciels ni faille de sécurité.

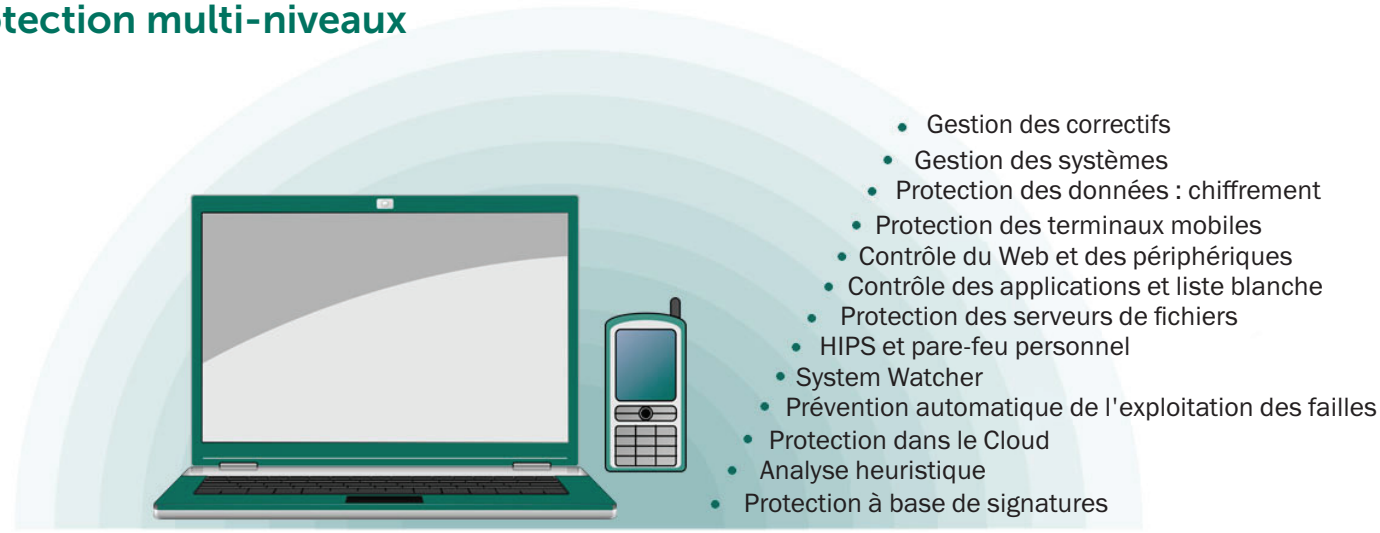
PUISSANTE SURVEILLANCE DES MENACES

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.

ADMINISTRATION 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 administration supplémentaire.

Protection multi-niveaux



Élimination et prévention inégalée des menaces nouvelle génération

Au centre de votre stratégie de sécurité se trouve le moteur de protection des terminaux le plus puissant et le plus efficace du secteur, comme le confirment en permanence les tests indépendants[1].

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 **basée sur plusieurs algorithmes** : détecte les programmes malveillants inconnus **et complète les technologies** traditionnelles basées sur les signatures.
- **Kaspersky Security Network (KSN) dans le Cloud** : facilite l'identification et le blocage des nouvelles menaces 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 System Watcher** : bloque les menaces inconnues en détectant les caractéristiques comportementales suspectes et restaure les fichiers clés si le système est impacté.
- **Système de prévention des intrusions basé sur l'hébergeur (HIPS)** : limite les activités et accorde les droits d'accès en fonction du niveau de confiance du logiciel.
- **Le pare-feu personnel** limite l'activité du réseau.
- **Network Attack Blocker** stoppe les attaques réseau.
- **Les serveurs de fichiers** sont également totalement protégés.

Contrôlez chaque terminal

Réduisez l'exposition au risque des terminaux tout en gagnant en productivité. Contrôlez l'accès de chaque terminal aux applications, sites Web et plug-ins en identifiant et bloquant les terminaux inappropriés, en régulant l'accès des terminaux non nécessaires et en favorisant les terminaux utiles et dignes de confiance.

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

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 de confiance que vous avez approuvées continuent de fonctionner avec fluidité.

LA CRÉATION DE LISTES BLANCHES FLEXIBLES DANS LE CLOUD

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

PARER LES DANGERS DE LA NAVIGATION SUR LE WEB

Le contrôle du Web surveille, filtre et contrôle chaque site Web 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 Web et les médias 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.

Protection des données grâce au chiffrement intégré

Le **chiffrement** puissant et transparent vis-à-vis des utilisateurs sécurise totalement les données sensibles 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.

1 Référence ici – Top3.

Supprimer les vulnérabilités grâce à l'application intelligente des correctifs

L'exploitation des vulnérabilités découvertes dans une application de confiance 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 des appareils mobiles** vous protège contre les menaces qui ciblent les données sensibles des mobiles, et contre celles qui exploitent les failles de sécurité des appareils des employés ou de l'entreprise pour infiltrer les systèmes.

Fonctionnalités incluses

- **Protection multi-niveaux puissante** contre les menaces pour toutes les principales plateformes mobiles.
- Technologie **anti-phishing** : bloque les liens dangereux figurant dans les messages et sur les pages Web, tandis que les filtres d'appels/sms empêchent les communications non souhaitées
- **Conteneurisation d'applications** : permet de conteneuriser, de chiffrer et d'empaqueter les données de l'entreprise sur les appareils personnels des employés.
- **Le contrôle du Web et le contrôle des applications,** pris en charge par KSN, bloquent l'accès aux sites Web et logiciels non autorisés.
- **Antivol** : comprend la suppression des données, le verrouillage de l'appareil, la localisation, la surveillance de la carte SIM, le « mugshot » et l'alarme, ce qui permet de rendre inutilisables les appareils égarés ou dérobés et d'effacer les données sensibles qu'ils contiennent.
- Détection et signalement des **appareils déverrouillés** afin que des mesures soient prises.
- **Gestion centralisée** : comprenant la fonctionnalité de gestion des applications et des appareils mobiles (MDM/MAM). Les politiques peuvent être déployées sur différents appareils fonctionnant sur toutes les principales plateformes à partir d'une interface unique.

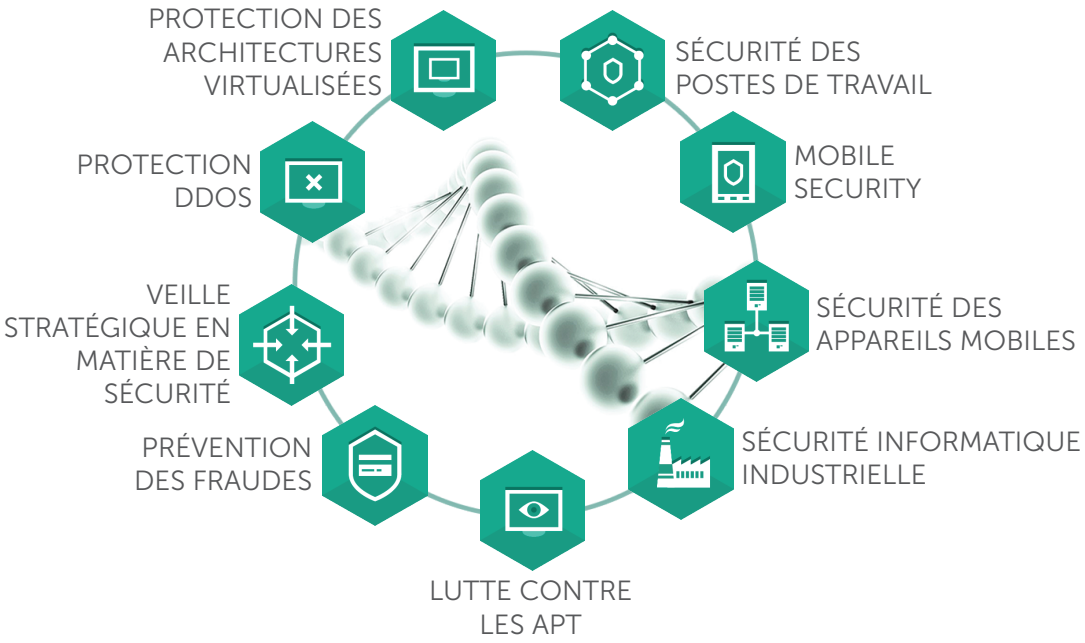
Optimisation de l'efficacité : gestion intégrée

Kaspersky Endpoint Security for Enterprise permet à vos équipes en charge de la sécurité de bénéficier d'une visibilité intégrale et d'un contrôle total sur chaque terminal mobile ou statique 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 entreprises 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 haut de gamme ou à source unique, Kaspersky Lab propose **de nombreuses solutions pour l'entreprise** qui se combinent ou fonctionnent en parfaite indépendance pour que vous puissiez faire votre choix en toute liberté sans sacrifier l'efficacité et les performances. Les solutions couvrant les serveurs, les infrastructures et les systèmes **virtuels** et **physiques** sont complétées par les solutions qui ciblent les **problèmes spécifiques au secteur**, tels que la fraude financière et les attaques de type déni de service (DDoS), ainsi que par notre gamme de **services de veille en matière de sécurité**.



Maintenance et assistance

Opérant dans plus de 200 pays, à partir de 34 bureaux répartis dans le monde entier, notre engagement permanent d'assistance globale (24h/24, 7j/7, 365 jours par an) se reflète dans nos offres **Maintenance Service Agreement (MSA)**. Nos équipes en charge des **services professionnels** sont prêtes à intervenir à tout moment pour que vous puissiez tirer le maximum 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 Enterprise Security for Endpoints/V 1.0/Nov 15/Global