KASPERSKY lab

Solution de protection des terminaux de nouvelle génération

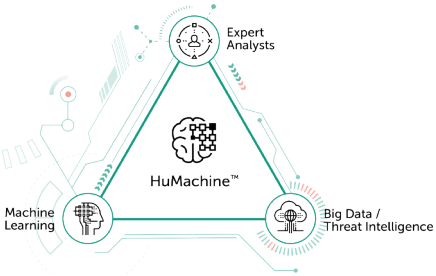
www.kaspersky.fr/small-to-medium-business-security
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Protection dans le cadre de votre stratégie de continuité d'activité

La technologie est une force transformatrice de l'entreprise, qui doit suivre le rythme ou stagner. Mais la technologie ouvre également la porte aux criminels. Le terminal est leur cible principale et la source de la plupart des problèmes. Au cours de l'année dernière, plus de 38 % des entreprises ont subi une cyberattaque, tandis que 39 % des attaques visant des terminaux protégés ont réussi. Dans cet environnement, les entreprises doivent être plus rusées que les cybercriminels qui les attaquent.

Tant que les cyberattaques seront menées par des êtres humains, leur prévention nécessitera l'association de l'intellect humain à des technologies novatrices. La solution de protection de Kaspersky Lab repose sur l'association de notre Threat Intelligence mondiale à des algorithmes de Machine Learning et à l'expertise des meilleurs spécialistes du secteur. Cette combinaison unique, que nous dénommons HuMachine™, est au cœur de nos produits.



En 2017, Kaspersky Lab a remporté le prestigieux prix **Platinum Customer Award de Gartner Peer Insights pour les plateformes de protection de terminaux**. Ce prix est la plus haute distinction possible sur le marché concurrentiel des plateformes de protection des terminaux. Nos applications pour terminaux sont le plus souvent classées aux trois premières places (90 %) selon des tests indépendants, comparativement à tout autre fournisseur.

Investir dans l'avenir

L'impact financier moyen d'une seule violation de données est estimé à 86 500 dollars pour une petite ou moyenne entreprise et à 992 000 dollars pour une grande entreprise. Les antivirus de nouvelle génération ne suffisent plus. Seule une solution multidimensionnelle garantissant une sécurité sur plusieurs niveaux technologiques et fonctionnels de l'infrastructure informatique de l'entreprise peut offrir la protection dont vous avez besoin. Une véritable sécurité des terminaux associe un éventail de techniques et technologies intelligentes pour protéger les entreprises contre toutes sortes de cybermenaces, sur n'importe quelle plateforme. En protégeant la totalité de votre réseau informatique, vous assurez la continuité de vos opérations.

Protégez vos ressources les plus précieuses avec des applications basées sur HuMachine™

Votre budget de sécurité informatique ne peut pas croître au même rythme que celui de votre entreprise. Les ressources doivent être optimisées pour répondre aux défis d'aujourd'hui et de demain.
Kaspersky Endpoint Security for Business, exploitant l'intelligence HuMachine™, protège contre les ransomwares, les vulnérabilités et les cybermenaces avancées. Optimisée en fonction des ressources, la solution est dotée de contrôles de sécurité performants, de fonctionnalités de gestion des vulnérabilités et des correctifs automatisées et d'un chiffrement intégré, le tout contrôlé à partir d'une console unique, à l'échelle du réseau d'entreprise.

Sécurité adaptative et flexible

Ce produit est compatible avec n'importe quel environnement informatique. Il emploie de nombreuses technologies de nouvelle génération éprouvées. Les capteurs intégrés et l'intégration au Endpoint Detection and Response (EDR) permettent de capturer et d'analyser des volumes importants de données pour assurer la détection des cyberattaques les plus obscures et les plus sophistiquées.

Sécurité tournée vers l'avenir pour les services informatiques externalisés

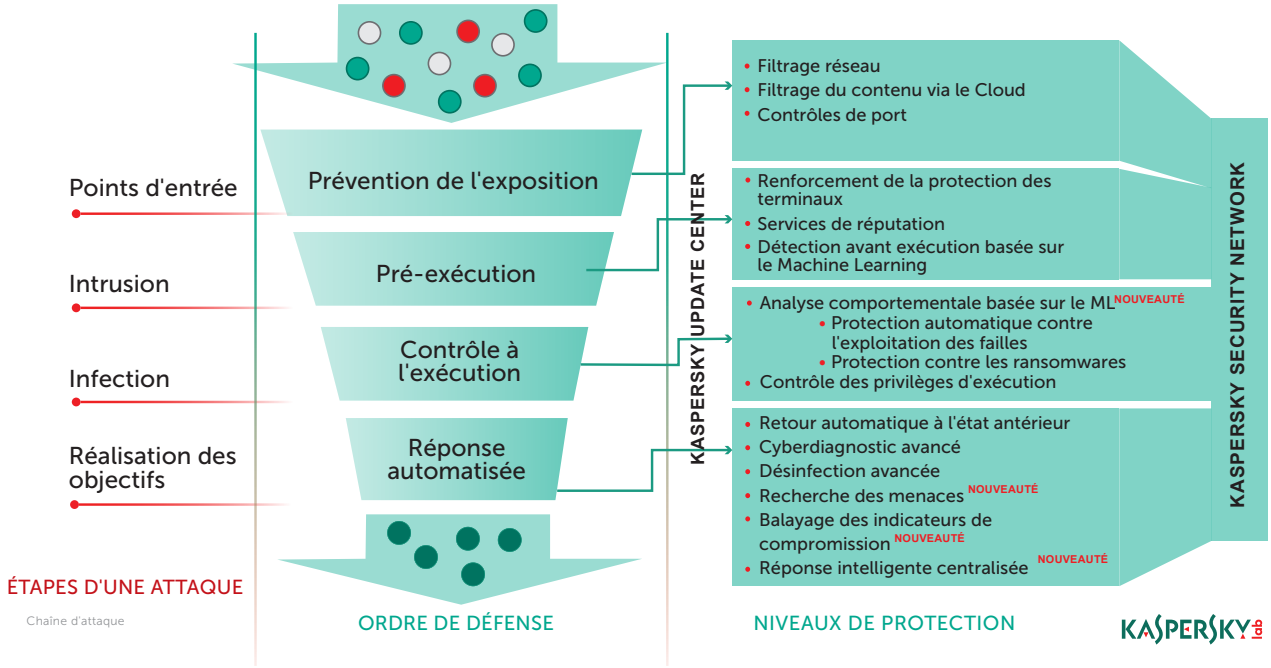
La location multiple intégrée, associée à la prévention des menaces, à la sécurité mobile, au chiffrement des données et à la gestion des vulnérabilités et des correctifs, permet aux fournisseurs de services gérés (MSP) d'ajouter la sécurité informatique à leurs offres.

Faible encombrement, performances élevées

Notre solution de sécurité la plus testée et la plus récompensée reposant sur notre approche HuMachine offre une protection optimale avec un impact minimal sur les ressources de l'ordinateur. Les composants sans signature assurent la détection des menaces, même sans mises à jour fréquentes.

Protection intégrale

Kaspersky Endpoint Security for Business utilise plusieurs technologies de nouvelle génération (telles que le renforcement de la sécurité des terminaux, l'analyse comportementale basée sur le Machine Learning, la prévention des vulnérabilités, etc.) afin de neutraliser la majorité des menaces avant qu'elles ne frappent les niveaux de protection avancés. Les fichiers suspects qui parviennent à atteindre le terminal sont détectés et bloqués.



Cette association de technologies avancées et d'une approche multiniveaux permet d'atteindre un équilibre parfait entre les performances et une protection efficace. Elles sont essentielles pour nous permettre d'atteindre l'un des plus hauts taux de détection du secteur, comme le démontrent continuellement les tests indépendants.

Plusieurs niveaux de protection pour

- Windows, Linux ou Mac
- Android et autres appareils mobiles
- Stockage amovible
- Serveurs Windows et Linux
- Serveurs de messagerie
- Passerelles Web
- Serveurs collaboratifs

Défense inégalée contre les menaces suivantes :

- Vulnérabilités logicielles
- Ransomware
- Code malveillant sur les appareils mobiles
- Les menaces inconnues
- Menaces sans fichier
- Attaques PowerShell et autres attaques à base de script
- Cybermenaces
- Menaces véhiculées par les emails
- Attaques par phishing
- Courriers indésirables

Protection contre les ransomwares et les Exploits

En se fondant sur des sources sans précédent de Threat Intelligence en temps réel et le Machine Learning, nos technologies évoluent constamment. Protégez l'ensemble de vos terminaux contre les vulnérabilités les plus récentes et conservez vos données ainsi que vos dossiers partagés à l'abri des menaces avancées et des ransomwares.

Blocage de la prise de contrôle de comptes

La détection comportementale met en œuvre un mécanisme de protection de la mémoire, qui protège les processus système critiques et empêche toute divulgation des informations d'identification des administrateurs et des utilisateurs.

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 sur les postes de travail et les serveurs. Le contrôle des applications intercepte le lancement de fichiers exécutables, de DLL et de scripts de commande exécutés par une variété d'interprètes. La détection comportementale et la prévention des vulnérabilités surveillent le comportement de l'application, bloquent les activités potentiellement malveillantes et protègent les applications légitimes de toute exploitation et utilisation par des logiciels malveillants. Les applications de confiance que vous avez approuvées continuent de fonctionner avec fluidité.

Neutralisation des rootkits

Les pirates utilisent des rootkits et des bootkits pour cacher leurs activités aux solutions de sécurité. La technologie anti-rootkit, partie intégrante de la solution de protection multiniveaux de nouvelle génération de Kaspersky Lab, permet de détecter les infections, même les plus profondément cachées, et de les neutraliser.

Détectez davantage d'attaques et d'intrusions, même les plus obscures

Les capteurs intégrés et l'intégration à Kaspersky Endpoint Detection and Response permettent la capture et l'analyse de grands volumes de données sur place, sans impact sur la productivité de l'utilisateur. La solution effectue une recherche des menaces avancées pour obtenir des preuves d'intrusion avec des indicateurs de compromission (IOC).

Prévention de l'exposition via les réseaux

Un programme malveillant utilisant une attaque par dépassement de la mémoire tampon peut modifier un processus en cours d'exécution dans la mémoire et exécuter ainsi son code. La protection contre les menaces réseau identifie les attaques et les vulnérabilités réseau et stoppe leur progression.

Maintenance et assistance

Nous intervenons 24 h sur 24, 7 jours sur 7 dans plus de 200 pays, à partir de nos 35 agences réparties dans le monde entier dans le cadre des offres d'assistance de notre contrat de maintenance et d'entretien (MSA). Nos services professionnels sont à votre écoute pour vous faire profiter au maximum des avantages de votre solution Kaspersky Lab, pour vous offrir une assistance au déploiement, ainsi qu'une prise en charge en cas d'incidents critiques.

Essai gratuit

Découvrez pourquoi seule la solution True Cybersecurity, associant flexibilité et facilité d'utilisation à la solution de surveillance **HuMachine™**, est en mesure de protéger votre entreprise contre tous les types de menaces. Rendez-vous sur cette page pour bénéficier d'une version d'évaluation gratuite de 30 jours de **Kaspersky Endpoint Security for Business**. À l'issue de l'essai, vous n'avez qu'à payer les frais de licence si vous décidez de l'acheter.

Au-delà de la protection des terminaux : maintenant et demain

Simplification de l'inventaire et de l'application de correctifs

La découverte des informations d'inventaire matériel et logiciel ainsi que la gestion de l'application des correctifs de vulnérabilités en temps voulu sont fastidieuses et chronophages. L'exploitation de vulnérabilités non corrigées est l'une des méthodes les plus courantes utilisées par les cybercriminels pour attaquer l'infrastructure informatique via un terminal unique. En allant au-delà du simple déploiement à distance des nouveaux logiciels tiers, l'évaluation automatisée de la vulnérabilité et la gestion des correctifs, fondées sur une surveillance 24 h/24 des vulnérabilités exploitées assurent la mise à jour des logiciels potentiellement vulnérables et permet à vos administrateurs informatiques de se consacrer à d'autres tâches.

Partage des données sécurisé par chiffrement

Le chiffrement certifié FIPS 140-2 transparent pour l'utilisateur sécurise intégralement les données confidentielles sur les appareils portables et sur site. Cette technologie intégrée permet de centraliser l'application du chiffrement des données de l'entreprise au niveau du fichier, du disque ou de l'appareil et d'activer le partage sécurisé des données sur votre réseau.

Prise en charge de scénarios distants et mobiles

Les données sont devenues accessibles à tout moment, transitant librement dans le périmètre. La sécurité mobile protège contre les menaces qui ciblent spécifiquement les données des mobiles et contre celles qui exploitent les failles des appareils pour infiltrer l'infrastructure. Le contrôle des appareils vous protège contre les conséquences de la perte des données sur des appareils portables non chiffrés ou non approuvés, ainsi que contre le téléchargement de données infectées à partir de l'appareil.

Optimisation de l'efficacité de la gestion pour toutes les plateformes

Une console unique vous offre une visibilité intégrale et un contrôle total sur chaque poste de travail, serveur ou appareil mobile, où qu'il se trouve et quoi qu'il fasse. Pratiquement adaptable à l'infini, la solution permet d'accéder aux licences, au dépannage à distance et aux contrôles du réseau. La gestion centralisée est complétée par l'intégration d'Active Directory, un modèle basé sur des rôles et des tableaux de bord intégrés.

Réglementation de l'accès aux données sensibles et aux appareils d'enregistrement

Notre solution restreint les privilèges d'application en fonction de niveaux de confiance attribués, limitant ainsi l'accès aux ressources comme les données chiffrées. Travailler par étape avec la base de données des réputations locale et dans le Cloud (KSN), ainsi qu'avec le système de prévention d'intrusion sur l'hôte permet de contrôler les applications et de limiter l'accès aux ressources système essentielles ainsi qu'aux appareils d'enregistrement audio et vidéo.

Arrêt des cybermenaces avant qu'elles n'atteignent les terminaux

En arrêtant la majorité des menaces entrantes au niveau de la passerelle, nous réduisons sensiblement l'impact du facteur humain et des caractéristiques sécurité des postes de travail en ne leur permettant pas d'atteindre les terminaux.

Une passerelle Internet sécurisée reste la première ligne de défense pour la majorité des scénarios de sécurité, malgré la progression des passerelles de sécurité dans le Cloud, Nos technologies de sécurité filtrent le trafic qui circule via les passerelles, en bloquant automatiquement les menaces entrantes avant qu'elles n'atteignent vos terminaux et serveurs. Cela réduit considérablement le risque d'exploitation de vulnérabilités, ainsi que les frais généraux opérationnels pour le personnel chargé de la sécurité informatique.

Augmentation de la productivité et réduction des menaces

L'Anti-Spam dans le Cloud de nouvelle génération de Kaspersky Lab détecte les courriers indésirables inconnus, même les plus sophistiqués, en réduisant au minimum les messages perdus en raison de faux positifs. La possibilité de réduire le temps perdu, ainsi que les risques liés au spam en stoppant ces derniers permet d'économiser les ressources système et humaines. La protection contre les programmes malveillants intègre plusieurs niveaux de sécurité proactive, notamment le Machine Learning et la Threat Intelligence dans le Cloud, pour filtrer les pièces jointes et les programmes malveillants, que ces derniers soient connus ou non, associés à des emails entrants.

Activation d'une collaboration sécurisée

Notre protection pour Microsoft SharePoint® comprend un outil de protection contre les programmes malveillants, ainsi que des capacités de filtrage des fichiers et des contenus afin d'aider votre entreprise à renforcer ses politiques de collaboration et d'empêcher le stockage de contenus inappropriés sur son réseau.

Kaspersky Endpoint Security for Business permet aux administrateurs de voir, surveiller, contrôler et protéger leur environnement informatique. Les outils et technologies de nouvelle génération sont proposés sous forme de versions évolutives, afin de répondre à vos nouveaux besoins en matière de sécurité à chaque stade du développement de votre entreprise.

Kaspersky® Total Security for Business

Les entreprises possédant des environnements informatiques développés associant des systèmes récents et hérités doivent ajuster leur sécurité pour différents systèmes. Notre solution de sécurité la plus complète pour les terminaux, l'infrastructure et les serveurs de collaboration vous le permet. Vous bénéficiez ainsi d'une sécurité sans faille et personnalisable en fonction de votre parc informatique.

Kaspersky® Endpoint Security for Business Advanced

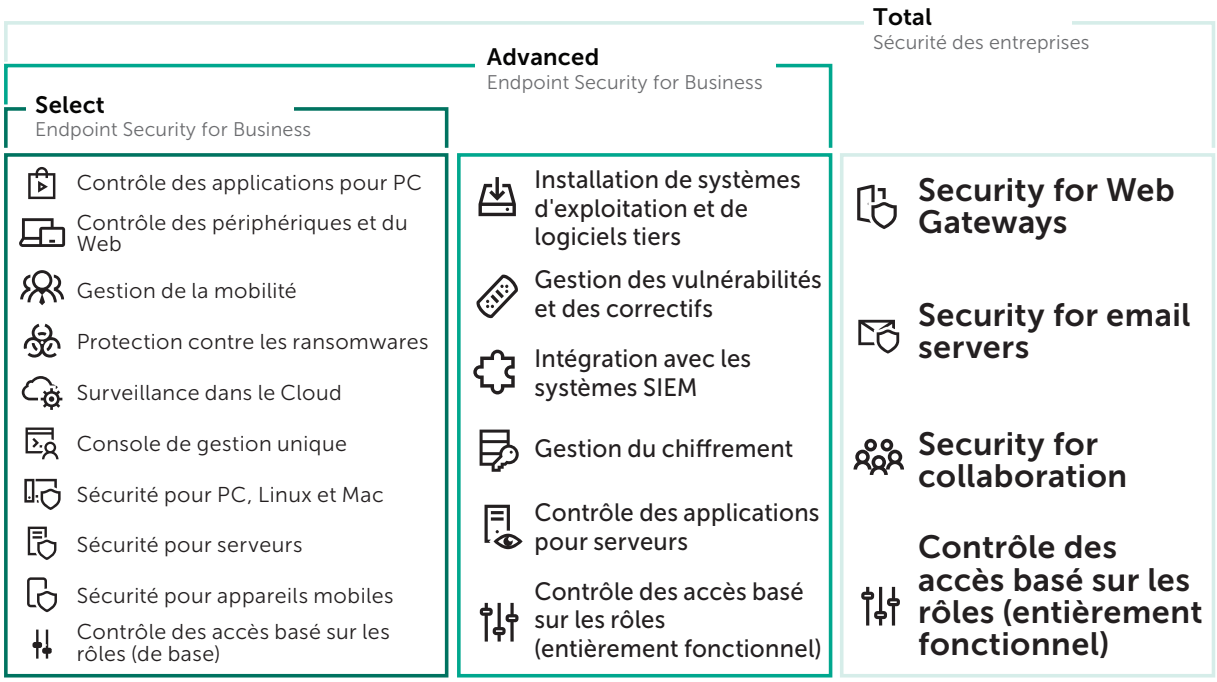
Pour une sécurité efficace qui protège votre entreprise, choisissez **Kaspersky Endpoint Security for Business Advanced**. Outre la sécurisation de tous vos terminaux et serveurs, cette solution propose des niveaux de sécurité pour protéger les données sensibles et éliminer les vulnérabilités, tout en simplifiant les tâches de gestion de systèmes.

Kaspersky® Endpoint Security for Business Select

Vos activités professionnelles devenant de plus en plus numériques, il devient nécessaire de protéger chaque serveur, ordinateur portable et appareil mobile. Nous offrons une sécurité de nouvelle génération au sein d'une solution unique, qui vous permet de protéger chaque terminal que votre entreprise exploite via une console de gestion flexible.

Quelle est la version la mieux adaptée à vos besoins ?

Quels que soient vos besoins informatiques, en constante évolution, **Kaspersky Endpoint Security for Business** est la solution idéale pour vous.



Renforcement de la sécurité lorsque vous en avez besoin

L'automatisation et la centralisation de la détection des vulnérabilités logicielles et de la gestion des correctifs permettent de se protéger contre les menaces les plus dangereuses, notamment les ransomwares. Pour les clients utilisant **Kaspersky Endpoint Security for Business Select**, cette automatisation est disponible via **le module complémentaire Kaspersky Vulnerability and Patch Management**.

Pour les clients utilisant Select, **le module complémentaire Kaspersky Encryption** permet un chiffrement intégral du disque au niveau des fichiers, en s'appuyant sur des algorithmes de chiffrement robustes et en assurant la prise en charge de l'authentification unique pour un accès immédiat aux fichiers chiffrés, ainsi que des cartes à puce/jetons pour l'authentification à deux facteurs. Il vous permet de chiffrer des fichiers et des dossiers stockés sur des disques locaux et amovibles.

Pour renforcer la sécurité sans complexité supplémentaire, il vous suffit d'activer la fonctionnalité requise définie dans Kaspersky Security Center.

Pourquoi mettre à niveau votre protection endpoint ?

Bénéficiez en permanence des dernières technologies, rapidement et en toute simplicité : un serveur, une console, un agent unique

Prenez en charge tous les processus métier via une intégration approfondie, basée sur un code unique, développée en interne

Évitez les coûts cachés et l'attribution de licences distinctes : un seul achat pour bénéficier de toutes les fonctionnalités dont vous avez besoin

Des fonctionnalités d'audit et de contrôle améliorés ; une gestion unifiée avec un accès basé sur les rôles

Comme Kaspersky Lab développe et perfectionne toutes ses technologies en interne, nos applications ont gagné en efficacité et en stabilité. Nous mettons tout en œuvre au sein de notre propre service de recherche et développement et intégrons de nombreuses innovations technologiques à nos produits. Voici quelques exemples :

- Machine Learning multiniveaux : utilisation de méthodes de Machine Learning à différents stades de la chaîne de frappe sur des terminaux et dans le Cloud.
- Recherche active des menaces découlant de l'intégration entre la protection des terminaux et les solutions Endpoint Detection & Response ou Anti Targeted Attack.
- Le mode Cloud exclusif pour les composants de protection offre une protection optimale avec un impact minimal sur les ressources de l'ordinateur et l'utilisation de la bande passante Internet.
- Prise en charge des conteneurs Microsoft Windows Server, de la sécurité du trafic externe et de la gestion de pare-feu.
- Fonctionnalité de contrôle des appareils et anti-bridging améliorée.
- Contrôle des applications amélioré avec la catégorie des certificats sécurisés et le mode de test de politiques.
- Une nouvelle interface utilisateur épurée permet de visualiser la protection multiniveaux, en indiquant l'état de la protection et l'efficacité des dernières technologies de Kaspersky Lab.

True Cybersecurity : une approche qui fait partie de notre ADN

Kaspersky Lab propose des solutions de cybersécurité performantes basées sur une Threat Intelligence leader, faisant partie intégrante de notre ADN et influençant toutes nos actions. Nous sommes une entreprise indépendante, ce qui nous permet d'être plus flexibles, de penser différemment et d'agir plus vite.

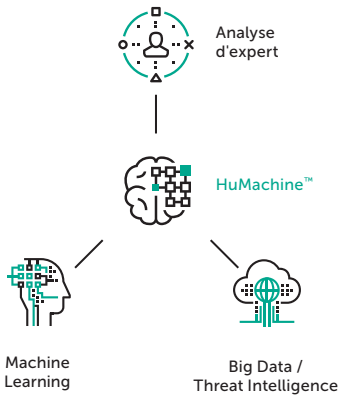
- **Notre expertise se retrouve à tous les niveaux de notre entreprise**, à commencer par notre direction, représentée par notre PDG, Eugene Kaspersky.
- Notre équipe d'analystes et de chercheurs au niveau mondial **(GReAT, Global Research & Analysis Team), composée d'experts en sécurité informatique, a détecté de nombreux programmes malveillants et attaques ciblées parmi les plus dangereuses au monde.**
- Notre initiative de **transparence mondiale** révolutionnaire est une autre preuve de notre engagement continu envers la protection des clients contre les cybermenaces, quelle que soit leur origine ou leur finalité.

Établissez votre conformité au RGPD avec True Cybersecurity

Kaspersky Lab sensibilise aux aspects liés à la cybersécurité du RGPD. Nos solutions permettent aux clients de réduire les risques de violation de données et de prévenir les incidents de sécurité. Nous offrons également aux responsables de la protection des données (RPD) de nos clients une visibilité accrue sur l'infrastructure surveillée.

Une vision globale - Solutions de sécurité informatique de Kaspersky Lab pour les entreprises

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 nombreux produits 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. Consultez notre site Web.



Solutions de sécurité Kaspersky Lab
Rechercher un partenaire près de chez vous : **https://kas.pr/kasperskypartnersfr**
Kaspersky for Business : **https://www.kaspersky.fr/small-to-medium-business-security**
True Cybersecurity : **www.kaspersky.fr/true-cybersecurity**
Actualités de la sécurité informatique : **www.securelist.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr