KASPERSKY lab

Solutions de sécurité Kaspersky Lab destinées aux entreprises 2018

#TrueCybersecurity

Solutions de sécurité Kaspersky Lab destinées aux entreprises 2018

La sécurité des entreprises à l'ère de la transformation numérique

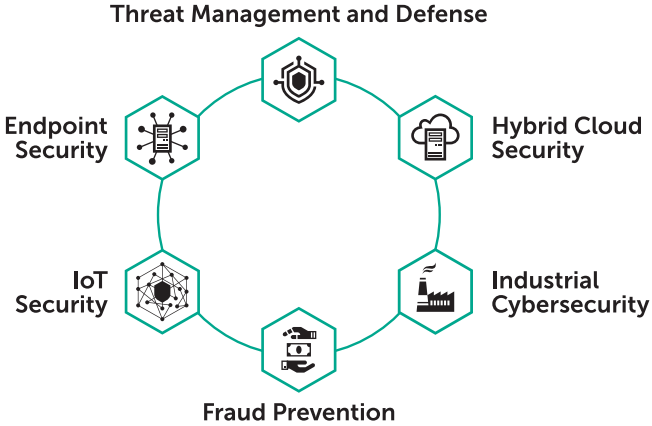
Le nombre de cyberattaques continue d'augmenter de façon spectaculaire, les attaques contre l'infrastructure des entreprises devenant de plus en plus professionnelles et hautement personnalisées. Il ne s'agit plus de savoir si vous serez attaqué, mais quand et à quelle vitesse, et comment vous pourrez vous rétablir.

Entre-temps, l'infrastructure informatique de l'entreprise est devenue de plus en plus complexe, car elle s'étend au-delà du périmètre organisationnel sur les appareils mobiles, les Clouds publics et les fournisseurs tiers. Si la transformation numérique apporte des avantages considérables en termes d'efficacité et d'agilité, elle apporte aussi de nouveaux défis en matière de sécurité. Assurer la continuité des affaires, protéger le rendement financier et les données de l'entreprise et des clients, voilà autant d'exigences considérables pour votre équipe de sécurité informatique et votre budget.

La nouvelle gamme de solutions pour les entreprises de Kaspersky Lab à la reflète les exigences de sécurité des entreprises d'aujourd'hui, en créant une plateforme de cybersécurité complète qui combine des capacités de protection entièrement évolutives pour les systèmes physiques, virtuels et basés dans le cloud, y compris les terminaux statiques et mobiles, les serveurs, les réseaux, le matériel et les logiciels spécialisés.

Une combinaison unique de technologies et de services performants permet à votre équipe de sécurité de prévenir la plupart des attaques, de détecter de nouvelles menaces et de prévoir les menaces futures, mais aussi de réagir aux incidents émergents, ce qui contribue ainsi à assurer la continuité opérationnelle et la conformité réglementaire.

Notre gamme se compose des solutions suivantes, toutes complétées par une vaste suite de services d'experts, de formations à la sécurité et d'assistance professionnelle :



Ces solutions et leurs composants technologiques s'imbriquent pour créer un cadre de sécurité adaptative. Cela permet la prédiction, la prévention, la détection et la réparation des menaces les plus avancées en matière de cybersécurité et d'attaques ciblées, pour favoriser la continuité et la résilience de l'entreprise, avec un impact minimal sur les performances.

Une véritable cybersécurité, assistée par une combinaison de machine learning et d'expertise humaine et soutenue par une Threat Intelligence à la pointe de l'industrie, qui offre une protection de haute performance, une visibilité et une gestion unifiées, ainsi qu'une prise en charge complète de votre transformation numérique.

La lutte pour votre liberté numérique

Vos données et votre vie privée sont attaquées par des cybercriminels et cyberespions, vous avez donc besoin d'un partenaire qui n'a pas peur de vous soutenir dans la lutte pour défendre les actifs de votre entreprise. Depuis 20 ans, Kaspersky Lab a découvert et vaincu toutes sortes de cybermenaces, qu'elles proviennent de « script kiddies » (pirates adolescents), de cybercriminels ou de gouvernements, du nord, du sud, de l'est ou de l'ouest. Nous pensons que le monde en ligne devrait être à l'abri des attaques et de l'espionnage commandité par les États, et nous continuerons à lutter pour un monde numérique véritablement libre et sécurisé.

Reconnu

Kaspersky Lab obtient régulièrement les meilleures notes dans de nombreux classements et études réalisés par des organismes indépendants.

- Évalué aux côtés de **80 fournisseurs bien connus** dans l'industrie
- **72 premières places** dans 86 tests en 2017
- **Classement aux 3 premières places*** dans plus de 90 % de l'ensemble des tests produits
- En 2017, Kaspersky Lab a reçu le **statut Platinum** du Gartner's Peer Insight** Customer Choice Award, pour le marché des plateformes de protection de terminaux

Notre équipe Global Research and Analysis Team (GReAT, équipe mondiale d'analyse et de recherche) a participé activement à la découverte et à la révélation de plusieurs attaques par programme malveillant parmi les plus importantes liées à des gouvernements et des organisations étatiques.

Transparent

Nous sommes totalement transparents et tâchons de vous faciliter encore davantage la compréhension de ce que nous faisons :

- Relocalisation d'une partie de notre infrastructure en Suisse
- Audit et certification de notre code source par un tiers de confiance
- Examen indépendant des processus internes
- Trois centres de transparence d'ici 2020
- Augmentation des récompenses « bug bounty » (primes pour la découverte de bugs) avec jusqu'à 100 000 USD offerts par vulnérabilité découverte.

Indépendant

En tant que société privée, nous sommes indépendants de toute considération commerciale à court terme et de l'influence institutionnelle.

Nous partageons notre expertise, nos connaissances et nos découvertes techniques avec la communauté de la sécurité, les prestataires de sécurité, les organisations internationales et les agences chargées de l'application de la loi du monde entier.

Les membres de notre équipe de recherche sont disséminés partout à travers le monde et comprennent certains des plus célèbres experts mondiaux de la sécurité. Nous détectons et neutralisons toutes les formes de menaces persistantes avancées, quelle que soit leur origine ou leur finalité.

* https://www.kaspersky.fr/top3
** https://www.gartner.com/reviews/customerchoice- awards/endpoint-protection-platforms

Endpoint Security

La principale plateforme de protection des terminaux multi-niveaux reposant sur des technologies de cybersécurité de nouvelle génération

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.

Lors de l'édition 2017 du Gartner Peer Insights Customer Choice Awards pour les plateformes de protection des terminaux**, nous avons été le seul fournisseur à obtenir un prix Platinum***.

*Le logo Gartner Peer Insights Customer Choice est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses sociétés affiliées et son utilisation ici fait l'objet d'une autorisation. Tous droits réservés. Les prix Gartner Peer Insights Customer Choice (https://www.gartner.com/reviews/customer-choice-awards/endpointprotection-platforms) sont déterminés par les opinions subjectives des clients utilisateurs finaux en fonction de leurs propres expériences, du nombre de critiques publiées sur Gartner Peer Insights et des notes globales pour un fournisseur donné sur le marché, comme décrit plus en détail ici : http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/ et ne sont en aucun cas destinés à représenter les opinions de Gartner ou de ses filiales.

La transformation numérique entraîne des risques supplémentaires

La complexité croissante de la plupart des réseaux informatiques d'entreprise peut créer des « lacunes de visibilité » où les menaces peuvent se cacher.

En moyenne, une attaque ciblée peut continuer à se cacher dans les systèmes cibles, sans jamais être détectée, pendant 214 jours.

Pendant cette période, la menace peut continuer à mener une série d'activités frauduleuses. Il est donc d'une importance vitale d'utiliser des outils efficaces qui permettent de détecter, de nettoyer et de réparer rapidement.

Malheureusement, malgré les affirmations incroyables de certains fournisseurs, il n'y a pas un seul produit de sécurité miracle qui puisse garantir une protection à 100 % contre tous les types de risques. De même, il n'y a pas de « solution unique ». La sécurité informatique est donc un processus constant d'évaluation de l'évolution des dangers, pour ensuite :

- adapter et mettre à jour les règles de sécurité et
- déployer de nouvelles technologies de sécurité

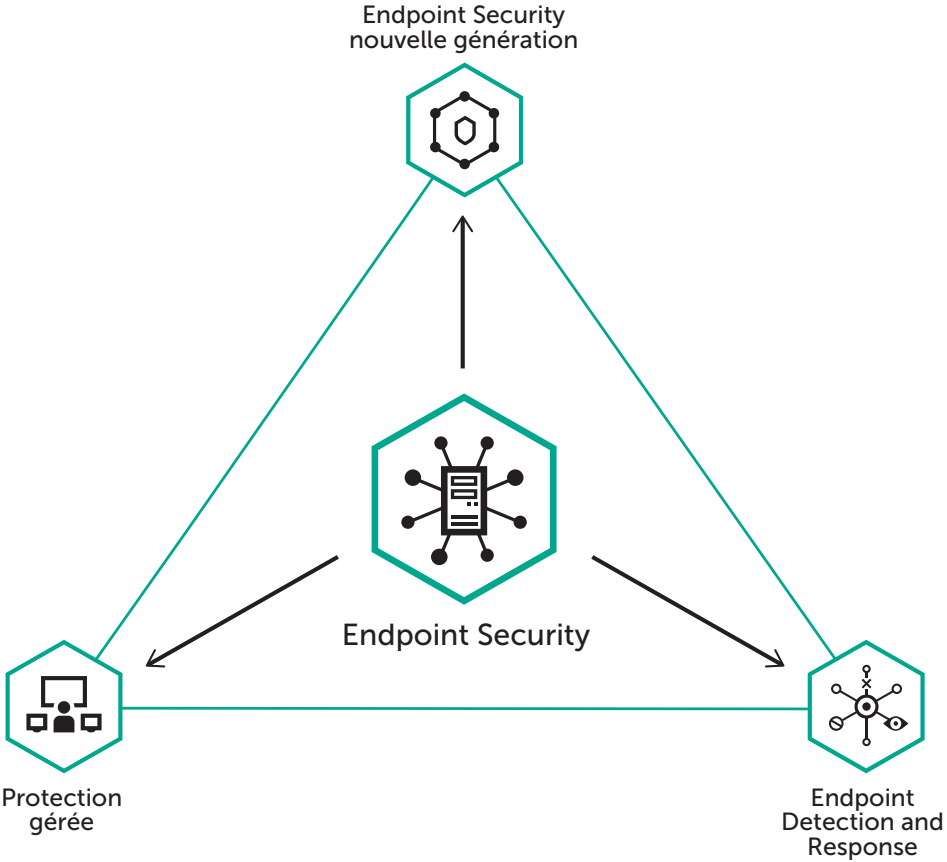
... pour faire face à de nouveaux risques.

Kaspersky Endpoint Security répond à ces besoins grâce à une plateforme de sécurité multi-niveaux fiable et éprouvée. Cette solution étroitement intégrée combine des capacités exceptionnelles de protection, de détection et d'intervention en cas d'incident, basées sur une veille stratégique mondiale inégalée et un machine learning de nouvelle génération, afin d'enrichir automatiquement votre SOC et d'améliorer vos capacités d'atténuation des risques. La protection de chaque terminal physique, virtuel et basé dans le Cloud est gérée par une seule console, ce qui améliore l'efficacité et réduit le coût total de possession.

Cette plateforme comprend :

- **Endpoint Security nouvelle génération**
  Une protection entièrement évolutive, basée sur notre moteur primé de Threat Intelligence et intégrant des contrôles granulaires, une protection contre les ransomwares et des technologies de prévention de l'exploitation des failles.
- **Endpoint Detection and Response**
  Fonctionne de manière proactive et arrête les menaces avant qu'elles ne provoquent des dommages coûteux en réagissant rapidement et efficacement aux incidents et violations de données.
- **Protection gérée**
  Une surveillance 24 h/24 des cybermenaces pesant sur votre organisation. et un service d'intervention en cas d'incident.

Solution Endpoint Security



Déroulement d'une attaque

La majorité des attaques se déroulent en quatre étapes distinctes :

- **Découverte** : identifier les points d'entrée appropriés pour l'attaque
- **Intrusion** : dans un terminal sur le réseau de l'entreprise
- **Infection** : elle se propage souvent à de nombreux endroits sur le réseau de l'entreprise
- **Mise en œuvre** : des actions malveillantes du cybercriminel.

Défense étape par étape

L'une des clés pour faire face à une attaque est d'avoir des défenses capables de fournir une protection à chacune des quatre étapes de l'attaque.

Prévention de l'exposition à la découverte
Pour bloquer l'accès aux points d'entrée potentiels

Protection contre les intrusions avant l'exécution
Pour détecter les menaces avant qu'elles ne puissent causer des infections

Processus post-exécution en cas d'infection
Pour détecter les comportements suspects et prévenir l'infection effectuant des actions malveillantes

Mise en œuvre d'une réponse automatisée
Pour aider l'entreprise victime à récupérer ses systèmes et ses données, et identifier comment éviter des attaques similaires à l'avenir.

Protection multi-niveaux... à partir d'un seul fournisseur

Nous fournissons des défenses pour toutes les étapes d'une attaque et à chaque étape, nous ne fournissons pas seulement une couche de défense, nous fournissons de multiples techniques de défense. Ainsi, nos clients bénéficient d'une protection multi-niveaux à chaque étape d'une attaque.

Étape de défense 1 : prévention de l'exposition
Nous bloquons les attaques aux points d'entrée potentiels.

Nos couches de protection comprennent :

- Filtrage réseau
- Filtrage du contenu via le Cloud
- Contrôles de port

Étape de défense 2 : protection avant l'exécution
Nous empêchons « l'intrus » de se lancer.

Nos couches de protection et services incluent :

- Renforcement de la protection des terminaux
- Services de réputation
- Détection avant l'exécution, basée sur le machine learning

Étape de défense 3 : contrôle à l'exécution
Nous recherchons de manière proactive tout comportement suspect sur les appareils connectés à votre réseau d'entreprise, y compris les appareils mobiles de vos salariés.

Nos couches de protection comprennent :

- Analyse comportementale, basée sur le machine learning, dont :
  - Protection automatique contre l'exploitation des failles
  - Protection contre les ransomwares
- Contrôle des privilèges d'exécution

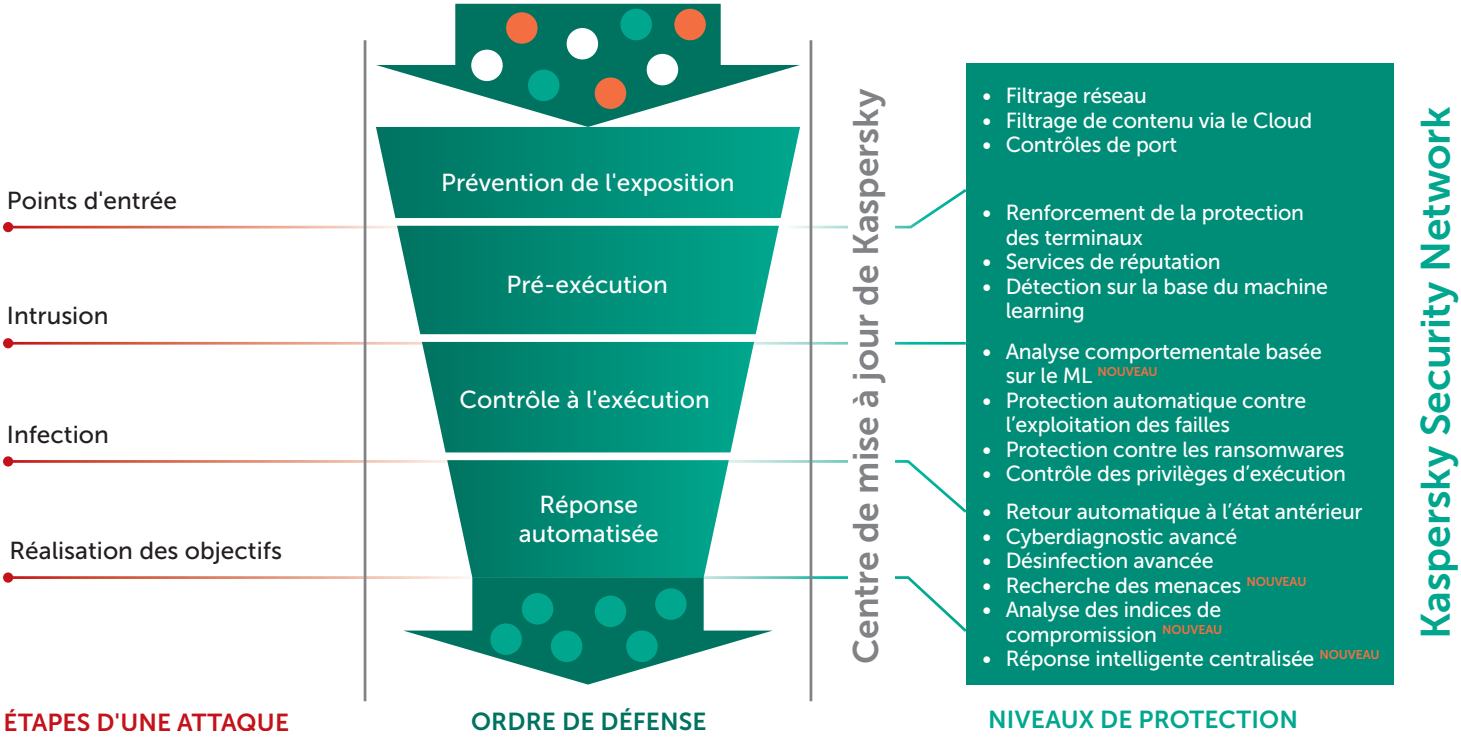
Étape de défense 4 : réponse automatisée
Si votre entreprise a été victime d'une attaque, nous vous aidons à faire face aux conséquences plus rapidement.

Nos technologies et services incluent :

- Retour automatique, pour restaurer les systèmes à leur état antérieur à l'attaque
- Cyberdiagnostic avancé
- Réparation de l'infection active
- Threat Hunting
- Balayage des indicateurs de compromission (IoC)
- Réponse intelligente centralisée

Notre protection multi-niveaux aide les entreprises à mieux se protéger contre les attaques ciblées dangereuses et les menaces persistantes sophistiquées en corrélant les résultats des différentes couches de défense, en identifiant les menaces qui peuvent passer à travers les défenses individuelles.

Chaîne d'attaque



Protection des appareils mobiles

Gestion et sécurité intégrées prenant en charge votre stratégie mobile

D'après notre enquête 2017, 38 % des entreprises ont subi des exploitations de faille ou une perte de données, les appareils mobiles étant le principal vecteur d'attaque.

1 700 000 $

Le coût moyen pour l'entreprise d'un incident de sécurité impliquant une exploitation de faille ou une perte de données via des appareils mobiles

Les logiciels et sites Web malveillants visant les appareils mobiles continuent à proliférer, de même que les attaques par phishing, tandis que les fonctionnalités des appareils mobiles sont encore en plein essor. En tant qu'outils de productivité importants à domicile et au bureau, les appareils mobiles représentent des cibles tentantes pour les cybercriminels. L'usage croissant d'appareils personnels dans le cadre professionnel (BYOD) élargit la gamme d'appareils et de plateformes utilisés sur le réseau de l'entreprise et représente une menace supplémentaire pour les administrateurs informatiques essayant de gérer et de contrôler leur infrastructure informatique.

Les appareils personnels des salariés constituent un risque pour l'entreprise

Les salariés utilisant leurs appareils mobiles dans un cadre professionnel, mais également personnel, augmentent les risques que votre sécurité informatique fasse l'objet d'une attaque. Une fois que les pirates ont accès à des informations personnelles non sécurisées sur un appareil mobile, il est assez simple d'accéder aux systèmes d'une entreprise et à ses données professionnelles.

Aucune plateforme n'est à l'abri

Les criminels ont toute une gamme de méthodes à leur disposition pour accéder sans autorisation aux appareils mobiles, et notamment les applications infectées, les réseaux Wi-Fi publics faiblement sécurisés, les attaques par phishing et les SMS infectés. Lorsqu'un utilisateur visite par inadvertance un site Web malveillant (ou même un site Web légitime infecté par un code malveillant), il met en danger la sécurité de son appareil et des données qui y sont stockées. La simple connexion d'un iPhone à un Mac pour charger sa batterie peut même entraîner le transfert d'une menace du Mac à l'iPhone (ces menaces sont communes à toutes les plates-formes mobiles les plus courantes : Android, iOS et Windows Phone).

La solution : Kaspersky Security for Mobile

Kaspersky Security for Mobile résout ces problèmes en fournissant une défense multi-niveaux contre les menaces mobiles (MTD) et des fonctions de gestion mobile. Ces capacités combinées permettent aux équipes de sécurité d'adopter une approche proactive de la gestion des menaces mobiles.

Toutes les fonctionnalités des terminaux et des appareils mobiles peuvent être gérées à partir de la même console, ce qui permet de lutter efficacement contre la cybercriminalité d'entreprise.

L'association d'un chiffrement fonctionnel et d'une protection contre les programmes malveillants permet à Kaspersky Security for Mobile de protéger les appareils mobiles de manière proactive plutôt que de simplement isoler un appareil et ses données.

Protection avancée pour appareils mobiles

Ce logiciel contre les programmes malveillants combine une protection contre les programmes malveillants à la Threat Intelligence dans le cloud et à des fonctions de machine learning afin de protéger les données stockées sur les appareils mobiles contre les menaces avancées.

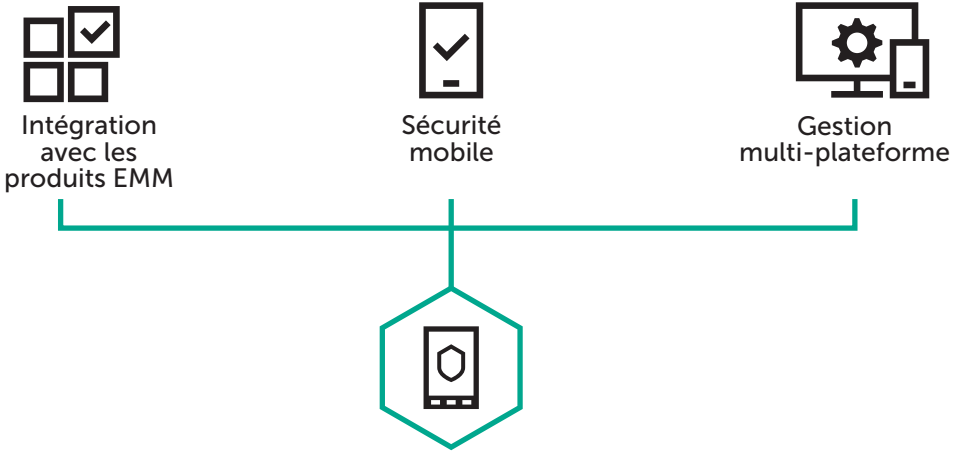
Solutions de contrôle du Web, anti-phishing et anti-spam

De puissantes technologies de contrôle Web, anti-phishing et anti-spam protègent contre les attaques de phishing et les sites Web, les appels et les textos indésirables.

Intégration aux plateformes EMM

Implémenter et gérer la sécurité mobile entièrement via votre console EMM (VMware AirWatch, Citrix XenMobile).

Protection avancée pour appareils mobiles



Hybrid Cloud Security

Une sécurité spécialement conçue pour vos environnements de cloud hybrides

Notre solution Hybrid Cloud Security offre une protection multi-niveaux unifiée pour les environnements basés dans le cloud. Quel que soit l'endroit où vous traitez et stockez des données professionnelles stratégiques (dans un cloud privé ou public, ou les deux), vous bénéficiez d'un équilibre parfait alliant agilité, sécurité permanente et efficacité optimale pour protéger vos données contre les menaces actuelles et futures les plus sophistiquées, sans compromettre les performances des systèmes.

La distribution simplifiée est réalisée grâce à l'intégration d'API natives, pour assurer le plus faible encombrement de ressources possible et des fonctionnalités précises sont fournies pour défendre les environnements cloud hybrides contre toutes les formes de cybermenaces. Le tout dans le cadre d'une administration et d'une gestion unifiée de la sécurité.

Cybersécurité de nouvelle génération pour tous les types de cloud

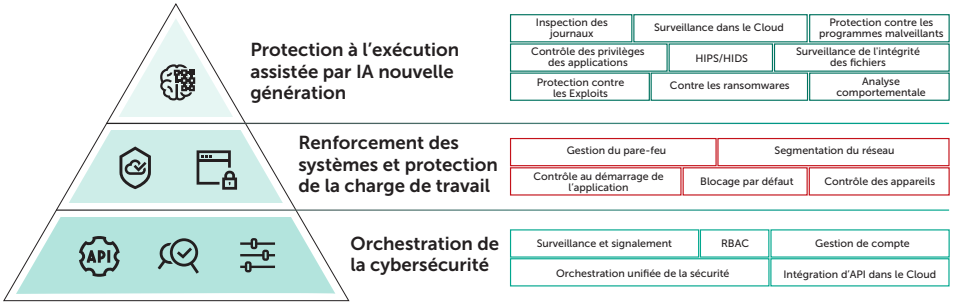
L'intégration avec les API du Cloud nous permet de fournir des technologies de cybersécurité à chaque charge de travail dans le Cloud.

Orchestration unifiée et transparence

La gestion, la flexibilité et la visibilité sont assurées par une console d'administration de la sécurité au niveau de l'entreprise. Transparence, car vous savez exactement ce qui se passe sur l'ensemble de la couche de sécurité de votre environnement de Cloud hybride. Cette visibilité, associée à la distribution entièrement automatisée des fonctionnalités de cybersécurité, permet l'orchestration transparente d'une sécurité meilleure et plus rapide sur l'ensemble de votre patrimoine basé dans le Cloud.

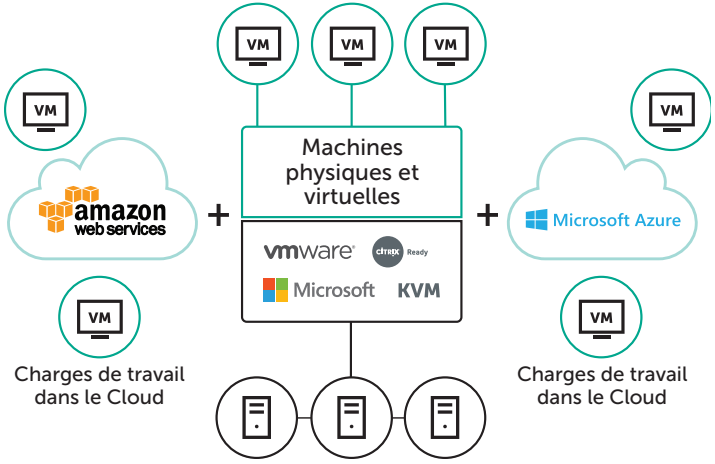
Pour des environnements cloud élastiques et sécurisés

Sécurité éprouvée pour les serveurs virtuels et physiques, le déploiement d'infrastructures de bureaux virtuels, les systèmes de stockage et même les systèmes de données. L'architecture brevetée et les capacités d'intégration intègrent la cybersécurité au cœur de votre environnement informatique, tout en maintenant l'efficacité opérationnelle des systèmes stratégiques de l'entreprise.



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security vous offre tout ce dont vous avez besoin pour construire un écosystème de cybersécurité parfaitement orchestré et adaptatif, offrant les fonctionnalités précises dont vos charges de travail multi-Cloud ont besoin, sans que l'efficacité des ressources et l'orchestration transparente soient affectées. Kaspersky Hybrid Cloud Security a été conçu pour protéger les applications et les données sur vos charges de travail physiques, virtuelles et Cloud, assurant la pérennité de votre entreprise et une conformité constante sur l'ensemble de votre environnement Cloud hybride.



Dans votre centre de données privé, où les charges de travail de l'entreprise sont exécutées sur des serveurs physiques ou virtuels ou même dans des environnements VDI, un certain nombre de considérations doivent être prises en compte dans le cadre d'une stratégie de transformation numérique réussie :

- **Accès et traitement sécurisés des données**, indépendamment de la plateforme de virtualisation ou de l'environnement physique sur lequel vos charges de travail s'exécutent
- **Interaction entre les couches informatiques et de sécurité** à l'aide d'API natives pour garantir des temps de réponse quasi nuls aux menaces avancées
- **Exploitation économe en ressources** améliorant les performances informatiques et maintenant la productivité des systèmes stratégiques de l'entreprise.

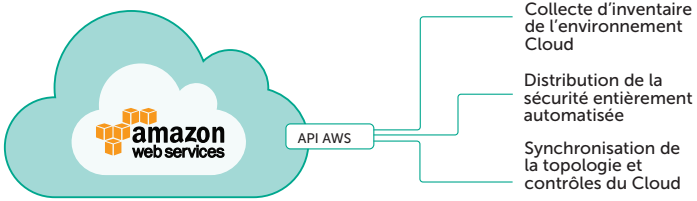
Kaspersky Hybrid Cloud Security offre une excellence éprouvée dans la protection des data centers à définition logicielle et construits sur les plateformes de virtualisation VMware NSX, Citrix XenServer et XenDesktop, MS Hyper-V et KVM, éliminant ainsi la complexité de la gestion des environnements à l'échelle de l'entreprise. L'intégration avec des fonctionnalités majeures via des API natives permet de répondre aux besoins de sécurité avec un impact quasi nul sur les performances des systèmes stratégiques.

- Sécurité intégrée sans agent pour VMware NSX pour vSphere, permettant aux couches de sécurité et informatique d'interagir pour une protection accrue.
- Protection brevetée basée sur un agent léger pour serveurs virtuels et plateformes VDI avec un fonctionnement à faible consommation de ressources et tolérant les pannes.
- Une sécurité traditionnelle multi-niveaux pour les serveurs physiques, intégrant des technologies de lutte contre les ransomwares, de prévention et de détection des comportements.

Cybersécurité automatisée pour les clouds publics

L'adoption croissante d'un modèle de services basé dans le cloud, où les ressources des centres de données privés s'étendent instantanément à la demande et, au besoin, dans des clouds externes, offre une flexibilité, une agilité et des avantages économiques sans précédent. Cependant, le modèle de responsabilité partagée en matière de sécurité dicte le besoin de fonctionnalités supplémentaires, permettant une couche de cybersécurité élastique qui couvre l'ensemble de votre environnement cloud et protège vos charges de travail Amazon Web Services (AWS) ou Microsoft Azure.

S'intègre avec Amazon Web Services (AWS)



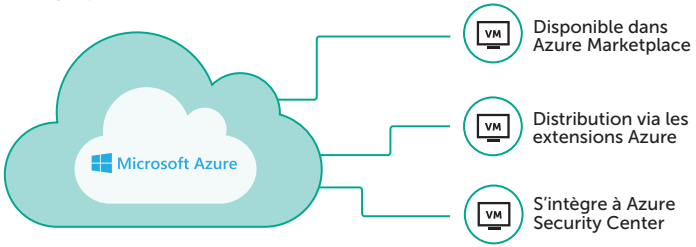
Kaspersky Hybrid Cloud Security défend les actifs basés dans le Cloud, en répondant à la nécessité de protéger tout ce qui est déployé dans le Cloud public dans le cadre de votre responsabilité partagée en matière de sécurité. Kaspersky Hybrid Cloud Security fournit une protection multi-niveaux qui s'intègre avec l'API Cloud et est disponible via les marchés en ligne pour fournir des techniques de cybersécurité primées à toutes les charges de travail dans le Cloud avec une plus grande agilité pour une expérience d'orchestration de cybersécurité multi-Cloud supérieure.

- Une cybersécurité performante protégeant vos charges de travail dans les Clouds publics, en tirant parti de l'intégration native via l'API Cloud avec Amazon Web Services (AWS) et les extensions Microsoft Azure.
- Complète les fonctionnalités de sécurité natives du Cloud et protège les applications, les systèmes d'exploitation, les données et les utilisateurs dans le Cloud, en prenant en charge la conformité RGPD.
- L'architecture intelligente et l'intégration d'API minimisent l'impact sur les ressources de cloud, en automatisant l'inventaire et la distribution de la sécurité.

Offre encore plus de protection

Nous complétons les outils natifs du Cloud avec la cybersécurité proactive, la prévention de l'exploitation de failles de sécurité, la surveillance de l'intégrité, l'inspection des journaux, les contrôles des applications et même la protection de l'exécution assistée par intelligence artificielle et les fonctionnalités de protection contre les ransomwares. Un produit pour lutter contre toutes les formes de cybermenace.

Conçu pour Microsoft Azure



Une sécurité imparable pour tous les Clouds

L'adoption du Cloud n'a jamais été aussi transparente et sécurisée. Avec Kaspersky Hybrid Cloud Security, l'intégration via des API natives facilite l'inventaire de l'infrastructure cloud publique et la distribution automatisée de la sécurité sur toutes vos instances dans AWS et Microsoft Azure.

Kaspersky Hybrid Cloud Security offre de multiples technologies de sécurité reconnues par l'industrie pour prendre en charge et simplifier la transformation de votre environnement informatique, en sécurisant votre migration du physique vers le virtuel et vers le Cloud, tandis que sa visibilité et sa transparence garantissent une expérience d'orchestration de sécurité sans faille.

Kaspersky Security for Storage

Kaspersky Security for Storage offre une protection robuste, haute performance et évolutive pour les données sensibles et précieuses résidant dans les systèmes de stockage en réseau NAS (Network Attached Storages) et les serveurs de fichiers de l'entreprise.

L'intégration en douceur grâce à des protocoles rapides, notamment ICAP et RPC, préserve l'efficacité des systèmes de stockage pour maintenir une protection fiable et efficace des ressources et une expérience optimisée pour l'utilisateur final. Une protection fiable en temps réel pour les systèmes de stockage qui inclut des fonctionnalités d'autodéfense pour une continuité optimale.

Protection des données fiable et transparente

- L'intégration native assure une flexibilité, une évolutivité et une efficacité opérationnelle remarquables, sans impact négatif sur les performances des systèmes de stockage de données et la productivité.
- Les technologies innovantes offrent les fonctionnalités de protection les plus avancées, une tolérance exceptionnelle aux pannes et même une protection contre les attaques de ransomware.

Sécurise vos données indépendamment de leur emplacement de stockage

- S'intègre de manière native avec les derniers NAS et fonctionne sur les serveurs de fichiers de l'entreprise
- Tous les fichiers de stockage de données sont sécurisés, sans qu'il soit nécessaire de vérifier les logiciels contre les programmes malveillants sur les terminaux ou les appareils mobiles
- Configuration flexible et granulaire pour les tâches d'analyse anti logiciels malveillants à la demande et en temps réel
- Capacités d'autodéfense pour une continuité opérationnelle optimale

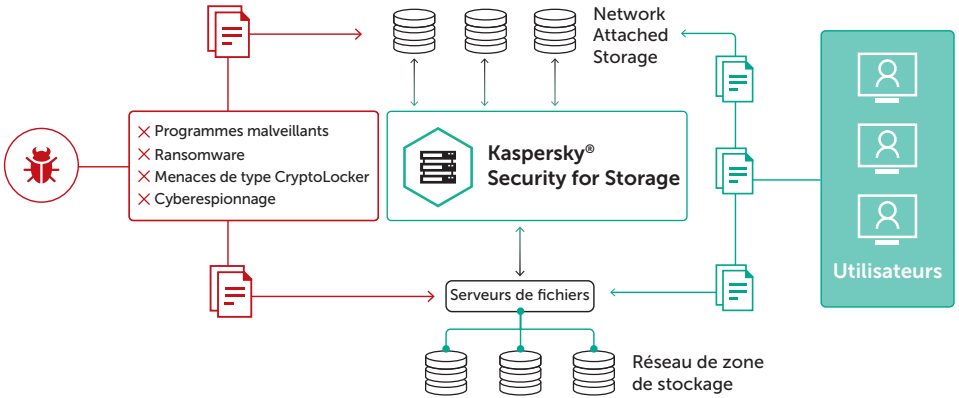
Lutte contre les logiciels malveillants et les ransomwares

- Notre moteur d'analyse contre les programmes malveillants primé défend tous les fichiers contre les attaques les plus avancées
- Protection en temps réel contre les logiciels malveillants pour les appareils NAS NetApp via FPolicy (lancé par Kaspersky Lab)
- Prise en charge d'une large gamme d'appareils de stockage, grâce à l'intégration via de multiples protocoles

Offre une sécurité à la fois légère et fiable

- L'intégration via l'API native signifie une plus grande sécurité avec moins d'impact sur la productivité de l'utilisateur final
- L'équilibrage de la charge et la tolérance aux pannes assurent une protection ininterrompue
- Visibilité totale de la cybersécurité des fichiers de données sur l'ensemble de votre infrastructure de stockage

Kaspersky Security for Storage peut être combiné avec Kaspersky Hybrid Cloud Security, pour obtenir la meilleure protection de sa catégorie sur les composants physiques et virtuels de votre centre de données d'entreprise.



Kaspersky DDoS Protection

L'impact financier d'une seule attaque DDoS peut se chiffrer entre 106 000 et 1 600 000 USD, selon la taille de l'entreprise. Le coût d'organisation d'une attaque DDoS ? Environ 20 USD...

Le coût de lancement d'une attaque de type déni de service distribué (DDoS) ayant baissé, leur nombre a augmenté. Les attaques sont devenues de plus en plus sophistiquées et difficiles à contrer. L'évolution de la nature de ces formes d'attaques appelle une protection plus rigoureuse.

Contrairement aux attaques par programme malveillant qui ont tendance à se propager automatiquement, les attaques DDoS reposent sur l'expertise et les connaissances humaines. Le cybercriminel effectue des recherches sur l'entreprise ciblée, en évaluant ses vulnérabilités et en choisissant soigneusement les outils d'attaque les plus appropriés pour atteindre son objectif. Au cours de l'attaque, les cybercriminels adaptent leurs tactiques en temps réel et sélectionnent différents outils afin d'optimiser les dommages qu'ils peuvent infliger.

Pour protéger votre entreprise contre les attaques DDoS, vous avez besoin d'une solution qui les détecte le plus rapidement possible.

La solution : Kaspersky DDoS Protection

Kaspersk DDoS Protection est une solution de protection et d'atténuation complète et intégrée, qui tient compte de chaque étape nécessaire pour défendre votre entreprise contre tous les types d'attaques DDoS. Trois options de déploiement sont disponibles : Connect, Connect+ et Control.

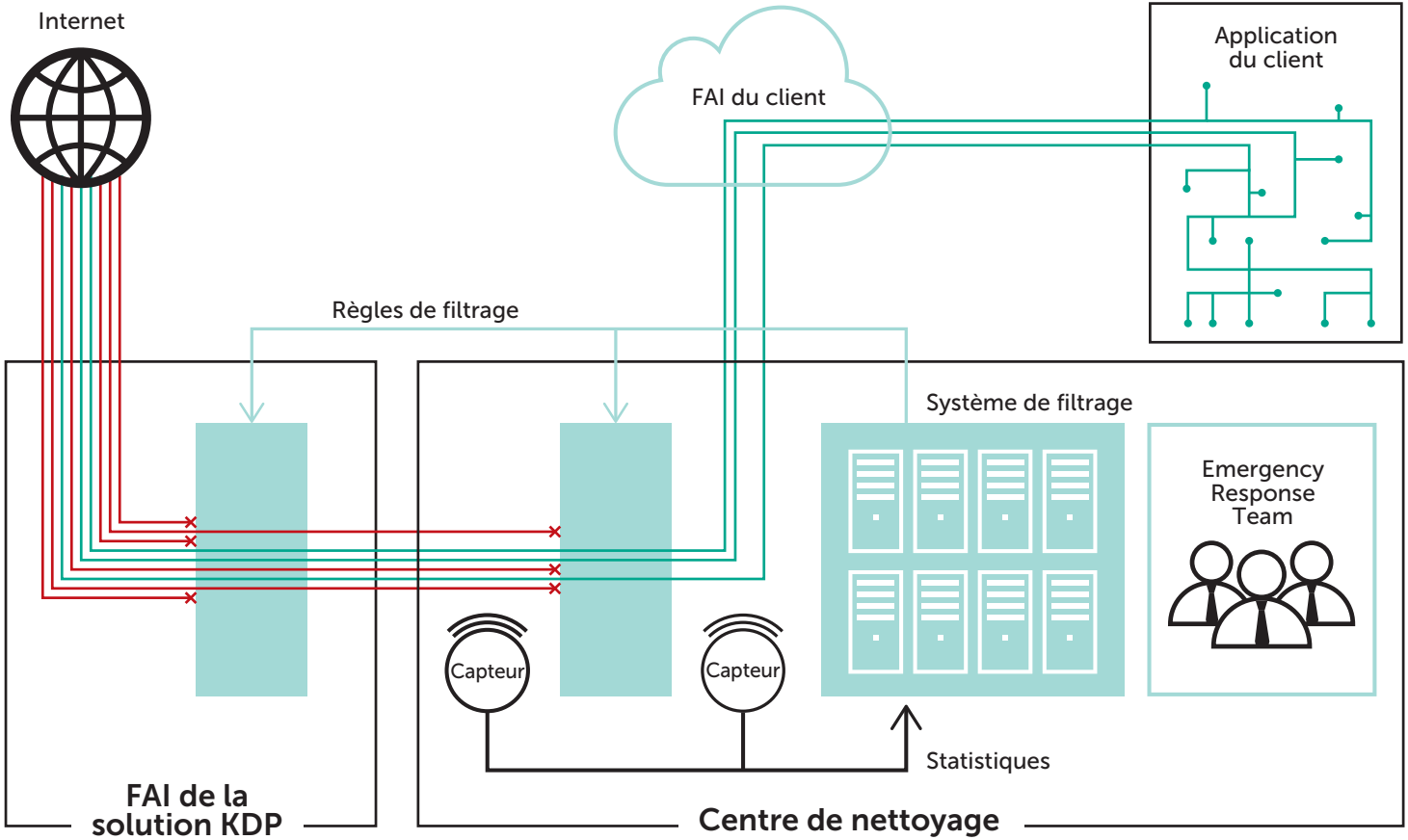
Dès qu'un scénario d'attaque possible est identifié, le centre d'opérations de sécurité de Kaspersky Lab reçoit une alerte. Dans le cadre des scénarios de déploiement Kaspersky DDoS Protection Connect et Connect+, la protection contre les attaques DDoS est automatiquement lancée. En parallèle, nos techniciens effectuent immédiatement une analyse détaillée afin d'optimiser l'atténuation en fonction de la taille, du type et de la sophistication de l'attaque DDoS. Avec la solution Kaspersky DDoS Protection Control, c'est vous qui décidez du moment auquel nous devons lancer les mesures d'atténuation en adéquation avec votre politique de cybersécurité, vos objectifs métier et votre infrastructure.

Grâce à notre capacité d'adaptation à différentes configurations, nous pouvons nous assurer de répondre entièrement aux besoins de votre entreprise et de ses ressources en ligne.

Architecture de Kaspersky DDoS Protection

Cette solution de défense complète offre :

- Protection complète de vos infrastructures réseau et de vos ressources en ligne essentielles
- Options de déploiement flexibles : Kaspersky DDoS Protection Connect, Connect+ et Control
- Centres de nettoyage hautement évolutifs dans toute l'Europe
- Système de surveillance des menaces DDoS en temps réel basé sur l'analyse de la sécurité du big data
- Protection rapide et assistance de l'équipe ERT 24 h/24 et 7 j/7 (Emergency Response Team).


Internet
FAI du client
Application du client
Règles de filtrage
Système de filtrage
Emergency Response Team
Capteur
Capteur
Statistiques
FAI de la solution KDP
Centre de nettoyage

Threat Management and Defense

Protection avancée et Threat Intelligence

La protection des infrastructures hautement numérisées pose de nouveaux défis importants pour les entreprises :

- Volume élevé de tâches manuelles requises pour l'intervention en cas d'incident
- Le sous-effectif de l'équipe de sécurité informatique et le manque d'expertise de haut niveau
- Trop d'événements de sécurité pour les traiter, les analyser, les trier et y réagir efficacement dans un délai limité
- Problèmes de confiance et de conformité du partage des données à mesure que la portée de l'infrastructure numérique s'élargit.
- Manque de visibilité et difficultés de collecte de données probantes pour l'analyse post-violation

Valeur commerciale de l'investissement dans la gestion des menaces et la défense :

- Réduction des dommages financiers et opérationnels causés par la cybercriminalité
- Complexité réduite grâce à une interface de gestion simple et axée sur les activités commerciales
- Réduction des coûts administratifs grâce à l'automatisation des tâches et à la simplification des processus de conformité en matière de sécurité
- Augmentation du retour sur investissement grâce à l'automatisation transparente de flux de travail sans interruption des processus commerciaux
- Réduction du risque de menaces avancées grâce à une détection rapide

La transformation numérique. Un nouveau rôle pour la cybersécurité

La transformation numérique est un facteur clé de la croissance de l'entreprise et offre aux entreprises de nouvelles opportunités, mais comporte en même temps des risques associés à la sécurité de l'infrastructure informatique, ainsi qu'à la conformité et à l'utilisation sans risque des données. Les attaques ciblées et les menaces complexes, notamment les menaces persistantes avancées (Advanced Persistent Threats ou APT), représentent désormais les risques principaux auxquels les grandes entreprises doivent faire face. Solution unifiée prenant en charge l'innovation accélérée dans la transformation numérique, **Kaspersky Threat Management and Defense** s'adapte aux spécificités de l'organisation et de ses processus en cours grâce à une combinaison unique de technologies performantes en matière de sécurité et de services de cybersécurité, ce qui vous permet de construire une méthodologie unifiée pour une protection complète de l'entreprise contre les menaces avancées et les attaques ciblées uniques.

En prenant en charge le développement ou le renforcement de la stratégie de gestion des menaces de l'organisation, Kaspersky Threat Management and Defense permet la collecte automatisée d'informations et de preuves numériques, simplifie la détection manuelle et automatise l'analyse des incidents, grâce au machine learning. La richesse des données fournies permet de mener des enquêtes complexes sur les incidents et fournit le soutien et l'expertise nécessaires pour contrer les menaces les plus sophistiquées.

Kaspersky Threat Management and Defense offre une combinaison unique de technologies et de services prenant en charge l'implémentation d'une stratégie de sécurité adaptative. Cette solution aide à prévenir la plupart des attaques, détecter rapidement de nouvelles menaces uniques, réagir instantanément en cas d'incidents et anticiper les menaces. Kaspersky Threat Management and Defense comprend les composants suivants :

- **Kaspersky Anti Targeted Attack** repose sur des technologies performantes en matière de veille stratégique et de machine learning, combinées à la surveillance des réseaux et des terminaux, à la technologie avancée des sandbox et à l'analyse axée sur la Threat Intelligence. Kaspersky Anti Targeted Attack fait le lien entre différents événements et hiérarchise les incidents pour aider les entreprises à détecter les attaques ciblées, les menaces avancées et les systèmes déjà compromis.

- **Kaspersky Endpoint Detection and Response** améliore la visibilité des menaces sur les terminaux en agrégeant automatiquement et en stockant de manière centralisée les données de cyberdiagnostic. Kaspersky Endpoint Detection and Response utilise la même interface que Kaspersky Anti Targeted Attack et le même agent que Kaspersky Endpoint Security, fournissant une approche multifacette pour révéler, reconnaître et découvrir des attaques ciblées complexes. L'accent est mis sur la détection des menaces grâce à l'utilisation de technologies avancées, la réaction rapide aux attaques et la prévention des actions malveillantes en découvrant les menaces sur les terminaux.

- Les **services de cybersécurité de Kaspersky Lab** offrent une assistance rapide et professionnelle au cours d'un incident mais également pour la suite, afin de réduire le risque de données compromises et minimiser les éventuels dommages financiers et de réputation. Notre gamme de services de cybersécurité comprend un vaste programme de formation en matière de sécurité, une Threat Intelligence constamment mise à jour, une réponse rapide aux incidents, des évaluations proactives de sécurité, des services de recherche manuelle des menaces entièrement externalisés et une assistance haut de gamme 24 h/24, 7 j/7.

En fonction des exigences du client en matière de capacités de prévention avancées et des exigences de son infrastructure spécifique, notamment la nécessité d'isoler complètement les données de l'entreprise, nous pouvons enrichir notre solution de gestion des menaces et de défense avec les produits suivants, pour vous offrir une approche véritablement intégrée et stratégique de l'atténuation des risques et une prévention des menaces avancées et des attaques ciblées :

- **Kaspersky Endpoint Security** est une plateforme de protection des terminaux multi-niveaux, basée sur des technologies de cybersécurité de nouvelle génération alimentée par la veille HuMachine, offrant des défenses flexibles et automatisées contre les menaces connues et inconnues les plus avancées, notamment les attaques sans fichiers et les ransomwares, grâce aux moteurs de machine learning, à la détection des comportements suspects, aux contrôles, à la protection des données et plus encore.

- **Kaspersky Secure Mail Gateway** fait partie d'une approche préventive des attaques ciblées et offre une prévention automatisée des menaces visant la messagerie ainsi qu'une protection exceptionnelle du trafic sur les serveurs de visant la messagerie contre les spams, le phishing et les menaces de logiciels malveillants génériques et avancés. Kaspersky Secure Mail Gateway fonctionne efficacement même dans les infrastructures hétérogènes les plus complexes et quel que soit le modèle de distribution du courrier utilisé : cloud, sur site, chiffré.

- **Kaspersky Private Security Network** fournit une base de données complète sur les menaces pour les réseaux et environnements isolés avec des restrictions strictes en matière de partage de données, ce qui permet aux entreprises de profiter de la plupart des avantages de la sécurité dans le cloud sans divulguer aucune donnée en dehors du périmètre contrôlé. Il s'agit d'une version totalement privée, locale et personnelle de Kaspersky Security Network pour les entreprises. Kaspersky Private Security Network apporte une réponse aux principaux problèmes de cybersécurité des entreprises sans qu'une seule donnée ne quitte le réseau local.

Kaspersky Anti Targeted Attack

En mettant en corrélation des événements issus de plusieurs niveaux, y compris le réseau, les terminaux et le contexte mondial de menaces, Kaspersky Anti Targeted Attack fournit une détection « quasiment en temps réel » des menaces complexes tout en générant des données d'analyses criminalistiques essentielles pour appuyer le processus d'investigation.

Kaspersky Anti Targeted Attack fournit aux entreprises :

- Une continuité d'activité totale, réalisée grâce à l'intégration de la sécurité et de la conformité aux nouveaux processus dès le départ
- Une visibilité sur l'informatique de l'ombre et les menaces cachées
- Une flexibilité maximale permettant un déploiement dans les environnements physiques et virtuels, là où la visibilité et le contrôle sont nécessaires
- L'automatisation des tâches d'enquête et d'intervention, l'optimisation de la rentabilité de votre sécurité, de votre réponse aux incidents et de vos équipes SOC
- Intégration étroite et simple avec les produits de sécurité existants, ce qui améliore les niveaux de sécurité globaux et protège l'investissement dans les anciens produits de sécurité.

Kaspersky Endpoint Detection and Response

Les produits traditionnels de sécurité des terminaux (par exemple, Kaspersky Endpoint Security) jouent un rôle vital dans la protection contre un grand nombre de menaces, comme les ransomwares, les logiciels malveillants, les botnets, etc. Cependant, pour se protéger contre un nombre encore plus élevé de cyberattaques avancées et d'adversaires intelligents, les entreprises doivent maintenant mettre en œuvre des niveaux de protection supplémentaires au niveau des terminaux, notamment des processus de détection et de réponse.

Kaspersky Endpoint Detection and Response aide les entreprises à :

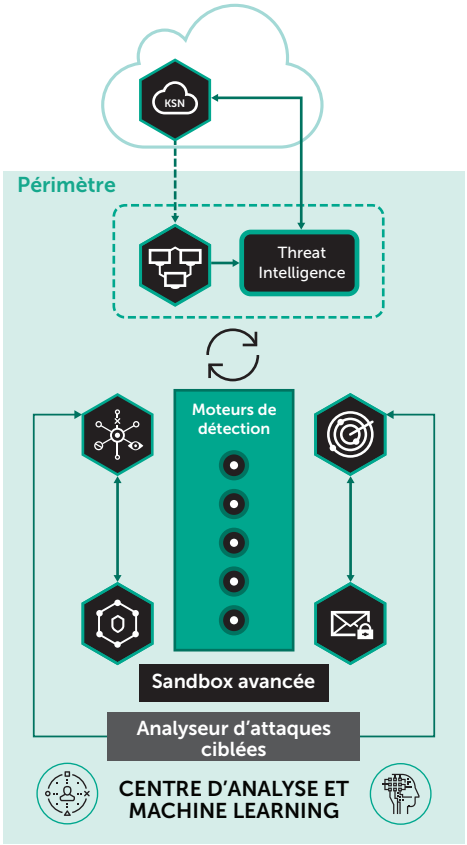
- Automatiser l'identification et la réponse aux menaces sans interruption de l'activité
- Améliorer la visibilité et la détection des menaces sur les terminaux, à l'aide de technologies avancées, incluant le machine learning, le sandboxing, l'analyse des indicateurs de compromission (IoC) et la surveillance des menaces
- Renforcer leur sécurité, en adoptant une solution de réponse aux incidents professionnelle et facile d'utilisation
- Établir des processus unifiés et performants de Threat Hunting, de gestion des incidents et de réponse.

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway est une solution automatisée de prévention des menaces présentes dans les courriers électroniques, offrant des technologies avancées pour protéger le trafic des emails de tout type, dans le cadre d'une approche unique de détection et de prévention des attaques ciblées. Kaspersky Secure Mail Gateway fournit une protection dans le cloud anti-spam, anti-phishing et anti-malware multi-niveaux avancée avec des capacités « zero-day » et de protection contre les exploits, alimentées par la Threat Intelligence, le machine learning et un sandboxing avancé pour fournir une approche automatisée multi-niveaux à la sécurité du courrier électronique.

Kaspersky Secure Mail Gateway fournit aux entreprises :

- Prévention automatisée des menaces connues, inconnues et futures
- Analyse de fichiers basée sur des signatures et hébergée dans le Cloud
- Analyse des fichiers à l'aide de méthodes de machine learning
- Notification rapide des incidents
- Amélioration continue de la cybersécurité des entreprises.



Kaspersky Private Security Network

Kaspersky Private Security Network est une version locale et entièrement privée de Kaspersky Security Network (KSN) permettant aux entreprises qui ne souhaitent pas divulguer des données en dehors de leur périmètre contrôlé de profiter de la plupart des avantages de la Threat Intelligence globale basée dans le cloud de Kaspersky Lab.

La technologie brevetée de Kaspersky Private Security Network :

- Permet d'accéder aux statistiques globales concernant les URL et les fichiers
- Classe les URL et les fichiers à l'aide de résultats d'analyses spécifiques des objets malveillants et figurant sur liste blanche
- Limite les dommages dus aux incidents de cybersécurité grâce à la prise en compte des menaces en temps réel
- Permet d'ajouter des résultats d'analyse des sources de menaces liées à chaque tiers et client (hachage de fichiers)
- Respecte les normes strictes en matière de confidentialité, de sécurité et de réglementation.

Services de cybersécurité

Threat Intelligence et expertise, offrant un niveau supplémentaire de cyberimmunité

Threat Intelligence Portal

En partageant nos informations les plus récentes avec nos clients, Kaspersky Lab offre aux entreprises une vue à 360° des méthodes, tactiques et outils utilisés par les cybercriminels, les aidant ainsi à se prémunir contre les cybermenaces modernes. Notre vaste gamme de services de Threat Intelligence garantit que votre centre d'opérations de sécurité (SOC) et/ou votre équipe de sécurité informatique est entièrement équipé(e) pour contrer les attaques, même les plus sophistiquées.

- **Flux d'informations sur les menaces.** Renforcez vos contrôles de sécurité (SIEM, IDS, pare-feu, etc.) et améliorez vos capacités de cyberdiagnostic grâce à nos données sur les cybermenaces constamment mises à jour, partagées dans une large gamme de formats et de méthodes de livraison
- Les **rapports de surveillance des menaces APT** permettent d'obtenir un accès exclusif et proactif aux descriptions des campagnes de cyberespionnage les plus sophistiquées, et notamment aux indicateurs de compromission (IOC) et aux règles YARA.
- Les **rapports Threat Intelligence financière** se concentrent sur les menaces visant spécifiquement les institutions financières, notamment les attaques ciblées, les attaques sur des infrastructures spécifiques (ex. distributeurs de billets/points de vente) et les outils développés ou vendus par des cybercriminels pour attaquer les banques, les sociétés de traitement des paiements, les distributeurs automatiques de billets et les systèmes de point de vente.
- **Rapports personnalisés sur les menaces.** Threat Intelligence personnalisée en fonction de votre entreprise ou pays provenant de sources propriétaires ou open comme le « Deep Web » et le « Dark Web ».
- **Kaspersky Threat Lookup.** Un portail Web vous offrant toutes les connaissances que Kaspersky Lab acquiert sur les indicateurs de menace et leurs relations.
- **Cloud Sandbox** vous permet de soumettre des fichiers suspects à Kaspersky Lab, d'obtenir une description détaillée du comportement du fichier et d'effectuer des enquêtes complètes et approfondies basées sur une intégration étroite avec Kaspersky Threat Lookup.
- **Suivi des attaques de phishing.** Notifications en temps réel sur les attaques par phishing dont vous ou vos clients êtes la cible.
- **Suivi d'activité des botnets.** Notifications en temps réel sur les attaques de botnets qui menacent vos clients et votre réputation.

Évaluation de la sécurité

Kaspersky Security Assessment Services : une analyse de la sécurité réalisée par des experts pour tester des systèmes d'information de tous les niveaux de complexité dans des environnements réels.

Test de pénétration
Simulation d'attaque axée sur la Threat Intelligence, pour révéler les vecteurs d'attaque potentiels et fournir une vue d'ensemble du système de sécurité de votre entreprise du point de vue d'un attaquant.

Évaluation de la sécurité des applications
Une recherche approfondie des failles métier et des vulnérabilités dans les applications de toutes sortes, depuis les solutions basées dans le Cloud jusqu'aux applications intégrées et mobiles.

Évaluation de la sécurité des systèmes de paiement
Analyse complète des composants matériels et logiciels des systèmes de paiement, pour révéler les scénarios de fraude potentiels et les vulnérabilités conduisant à des manipulations de transactions financières.

Évaluation de la sécurité du SCI
Modélisation des menaces spécifiques et évaluation de la vulnérabilité des systèmes de contrôle industriel et de leurs composants, pour vous donner un aperçu de votre surface d'attaque actuelle et de l'impact potentiel d'une attaque sur votre entreprise.

Évaluation de la sécurité des systèmes de transport
Une recherche spécialisée axée sur l'identification des problèmes de sécurité liés aux composants essentiels à la mission des infrastructures de transport modernes, de l'automobile à l'aérospatiale.

Évaluation des technologies intelligentes et de la sécurité de l'IoT
Une évaluation détaillée des appareils hautement interconnectés d'aujourd'hui et de leur infrastructure back-end, pour révéler les vulnérabilités des couches micrologicielles, réseau et applications.

Threat Hunting

Des techniques proactives de recherche de menaces menées par des professionnels de la sécurité hautement qualifiés et expérimentés, pour découvrir les menaces avancées qui se cachent au sein de l'entreprise.

- **Kaspersky Managed Protection**
  Service de contrôle 24 h/24, 7 j/7 et analyse constante de vos données de cybermenaces par des experts de Kaspersky Lab.
- **Découverte d'attaques ciblées**
  Une offre complète permettant d'identifier de manière proactive les signes actuels ou antérieurs de compromission et de répondre aux attaques manquées.

Réponse aux incidents

Les services de réponse aux incidents de Kaspersky Lab sont fournis par des analystes et des chercheurs chevronnés en cyberintrusions. Toute la force de notre expertise mondiale peut être mise à contribution pour résoudre votre incident de sécurité.

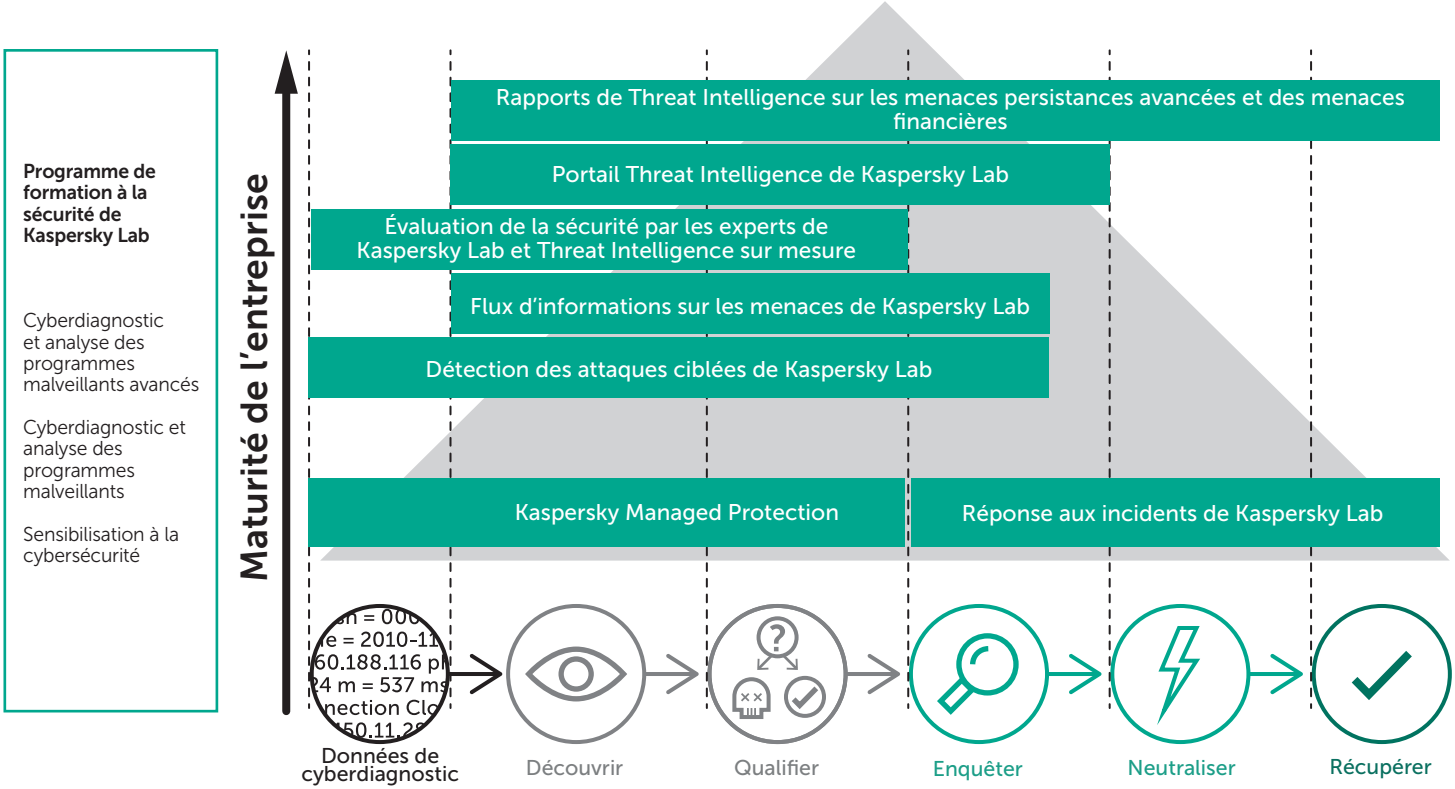
- **Réponse aux incidents.** Ce service couvre le cycle complet d'investigation sur les incidents pour éliminer complètement la menace qui pèse sur votre entreprise.
- **Cyberdiagnostic.** Analyse des preuves numériques relatives à la cybercriminalité avec création d'un rapport complet comprenant l'ensemble des conclusions.
- **Analyse des programmes malveillants.** Pour obtenir une visibilité complète du comportement et du fonctionnement des programmes malveillants spécifiques.

Formation à la sécurité

Nous proposons un ensemble de formations qui couvrent de nombreux sujets, des principes de base de la sécurité aux techniques et outils avancés utilisés dans les processus de cyberdiagnostic en passant par l'analyse des programmes malveillants et la réponse aux incidents. Il permet aux entreprises d'approfondir leurs connaissances en matière de cybersécurité dans ces domaines.

- **Cyberdiagnostic :** Les formations sont destinées à combler des lacunes en termes d'expérience : développez et renforcez vos compétences pratiques de veille et d'analyse des différents types de données pour identifier la chronologie et les sources des attaques.
- **Analyse avancée des programmes malveillants et reverse engineering :** Les formations apportent les connaissances nécessaires pour analyser des logiciels malveillants, recueillir des indicateurs de compromission, créer des signatures pour identifier les machines contaminées et restaurer des fichiers et des documents infectés/chiffrés.
- **Réponse aux incidents :** Les formations guideront votre équipe interne à travers toutes les étapes du processus de réponse aux incidents pour lui apporter les connaissances nécessaires pour une résolution efficace.
- **Détection efficace des menaces avec YARA :** Les participants apprendront comment rédiger les règles YARA les plus efficaces, comment les tester et les améliorer au point d'identifier des menaces jusque-là indétectables avec d'autres méthodes.

Kaspersky Cybersecurity Services



Sensibilisation à la cybersécurité

Créer un environnement informatique d'entreprise sécurisé grâce à la formation sous forme de jeux

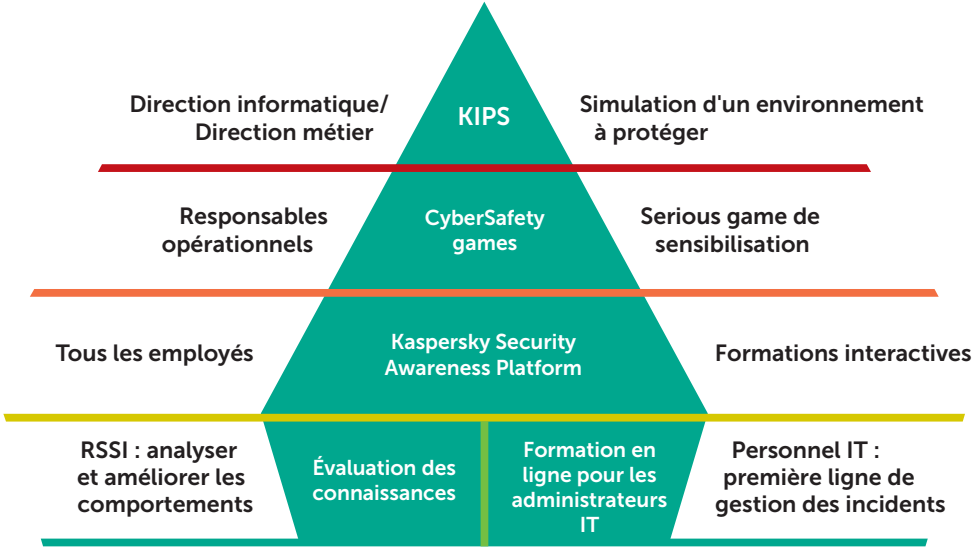
En moyenne, les entreprises doivent payer environ 1 155 000 $ pour se remettre d'attaques causées par des salariés négligents ou mal informés, tandis que les PME dépensent 83 000 $. Plus de 80 % des incidents informatiques sont dus à l'erreur humaine. À elles seules, les attaques de phishing coûtent jusqu'à 400 $ par salarié et par an.

Les entreprises perdent des millions pour se remettre d'incidents provoqués par le personnel, mais l'efficacité des programmes de formation traditionnels visant à prévenir ces problèmes est limitée et, bien souvent, ils ne réussissent pas à susciter la motivation et le comportement escompté.

Kaspersky Lab propose une gamme de produits de formation sur ordinateur qui utilisent les techniques d'apprentissage modernes et conviennent à tous les niveaux de la structure de l'entreprise. Notre programme de formation a déjà prouvé son efficacité, à la fois auprès de nos clients et de nos partenaires:

- Jusqu'à 90 % de diminution du nombre d'incidents
- Réduction de 50 à 60 % des pertes monétaires potentielles associées aux risques de cybersécurité
- Jusqu'à 93 % de probabilité que les connaissances soient utilisées au quotidien
- 86 % des participants recommanderaient cette formation à leurs collègues.

Produits pédagogiques de sensibilisation à la sécurité Kaspersky



Approche récompensée

- **Développer un comportement, et non uniquement transmettre des connaissances** : la méthode d'apprentissage inclut le jeu, l'apprentissage par la pratique, la dynamique de groupe, la simulation d'attaques, des parcours pédagogiques, le renforcement automatique des compétences, etc. De ce fait, les habitudes comportementales sont renforcées et les améliorations en termes de cybersécurité sont durables ;
- **Contenu pratique et sérieux** (basé sur la puissance de la R&D de Kaspersky Lab) présenté sous la forme d'un ensemble d'exercices interactifs adaptés afin de répondre aux besoins de l'entreprise et aux préférences en termes de format et de durée des différents niveaux de l'entreprise : cadres supérieurs, responsables hiérarchiques et employés ;
- **Évaluation en temps réel, gestion du programme sans effort** : le logiciel de formation conçu à cet effet offre des sessions de formation de manière automatique, des évaluations des compétences et du renforcement via des simulations répétées d'attaques de phishing et l'auto-inscription dans les modules de formation. Les autres formations et serious games peuvent être dispensés par des partenaires de Kaspersky Lab ou par les propres équipes du client (le support et les programmes de formation sont fournis par Kaspersky Lab).

Comment ça marche

- La formation aborde un large éventail de questions de sécurité : fuite de données, ransomwares, attaques de programmes malveillants sur Internet, utilisation sécurisée des réseaux sociaux et sécurité des appareils mobiles.
- La méthodologie d'apprentissage continu permet de renforcer les compétences de manière constante et de susciter la motivation au sein de l'entreprise.
- Les formations dédiées aux différents niveaux et fonctions de l'entreprise créent une culture de la cybersécurité collaborative, partagée par tous et pilotée par la direction.
- La formation inclut des outils de reporting et d'analyse qui évaluent les compétences et la progression de l'apprentissage des salariés, ainsi que l'efficacité des programmes au niveau de l'entreprise.
- Les plans pédagogiques et les bonnes pratiques fournis par Kaspersky Lab facilitent la mise en œuvre des programmes et permettent aux équipes T&D et de sécurité informatique du client de tirer le meilleur parti des initiatives de sensibilisation à la sécurité.

Industrial Cybersecurity

Protection spécialement conçue pour les environnements industriels

S'il suffisait auparavant d'isoler les processus industriels du monde extérieur pour offrir un niveau de protection adéquat, ce n'est plus le cas aujourd'hui. À l'ère de l'industrie 4.0, la plupart des réseaux industriels non essentiels sont accessibles via Internet, que ce soit par choix ou non.

Les attaques malveillantes dans les environnements industriels ont considérablement augmenté ces dernières années. Depuis trois ans, le risque d'interruption des activités et de perturbation de la chaîne d'approvisionnement occupe la première place des préoccupations des entreprises au niveau mondial ; le risque de cyberincident est d'ailleurs la principale crainte qui émerge de cette tendance. Pour les entreprises utilisant des systèmes industriels ou des systèmes d'infrastructure critiques, les risques n'ont jamais été aussi élevés.

Les conséquences de la sécurité industrielle vont bien au-delà de la protection de l'entreprise et de sa réputation. Dans bien des cas, de nombreux facteurs écologiques, sociaux et macroéconomiques importants sont à prendre en compte lorsqu'il s'agit de protéger les systèmes industriels contre les cybermenaces. Chaque infrastructure critique doit donc bénéficier du plus haut degré de protection possible pour contrer un éventail de menaces qui ne cesse de se développer.

Parallèlement, les environnements industriels ont besoin d'une solution intégrée qui maintient la disponibilité des processus industriels en détectant et prévenant les actions (intentionnelles ou accidentelles) susceptibles de provoquer une interruption ou une suspension des processus essentiels.

La solution : Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity est une gamme de technologies et de services conçus pour sécuriser tous les niveaux de l'industrie (serveurs SCADA, HMI, postes de travail des ingénieurs, API, connexions réseau et personnel) sans répercussion sur la continuité et la cohérence du processus industriel. Les paramètres polyvalents et flexibles de la solution permettent de configurer cette dernière pour répondre aux exigences et besoins uniques de chaque installation industrielle.

La solution a été développée pour protéger les infrastructures stratégiques, s'appuyant sur différents systèmes de contrôle industriels. La flexibilité et la portée de Kaspersky Industrial CyberSecurity permettent aux entreprises de configurer leur solution 100 % conforme aux exigences de leur environnement industriel. La configuration optimale des services et technologies de sécurité est déterminée via un audit complet de l'infrastructure réalisé par les experts de Kaspersky Lab.

L'approche de Kaspersky Lab en matière de protection des systèmes industriels repose sur un savoir-faire de plus de dix ans dans la découverte et l'analyse de certaines menaces industrielles parmi les plus sophistiquées au monde. Notre compréhension et nos connaissances approfondies de la nature des vulnérabilités des systèmes, associées à notre étroite collaboration avec les principales agences industrielles, gouvernementales et chargées de l'application de la loi, notamment Interpol, le Consortium pour la promotion de l'Internet industriel (Industrial Internet Consortium, IIC), divers fournisseurs ICS et organismes de réglementation, nous ont permis de jouer un rôle de leader pour répondre aux exigences uniques de l'industrie en matière de cybersécurité.

Cette solution hautement spécialisée :

- assure une approche globale de la cybersécurité des environnements industriels
- propose le cycle complet de services de sécurité, de l'évaluation de la cybersécurité à la réponse aux incidents
- offre des technologies de sécurité uniques spécialement développées pour les systèmes industriels
- réduit les temps d'arrêt et les retards au niveau des processus industriels.

Kaspersky Industrial CyberSecurity

Technologies

Détection des anomalies (DPI)

Intégration avec les autres systèmes

Protection contre les programmes malveillants

Contrôle de l'intégrité

Administration centralisée

Investigation des incidents

Système de détection des intrusions

Services

Formation et veille stratégique

- Formation à la cybersécurité
- Programmes de sensibilisation
- Threat Intelligence

Services d'experts

- Évaluation de la cybersécurité
- Intégration de la solution
- Maintenance
- Réaction en cas d'incident

Fraud Prevention

La solution avancée pour une expérience utilisateur transparente et une prévention proactive de la fraude en temps réel

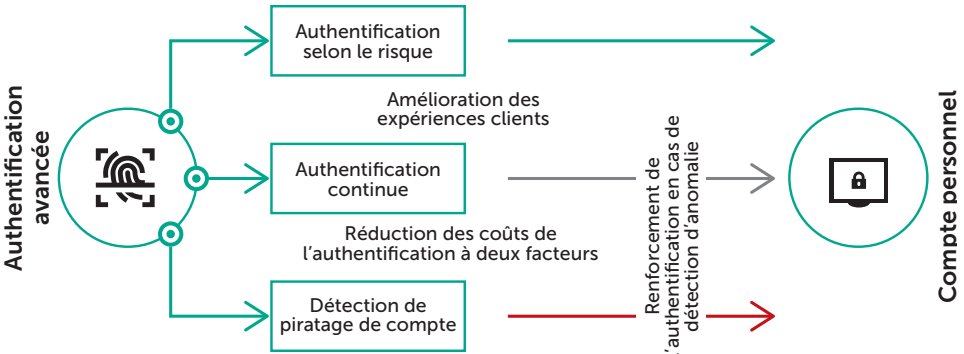
La transition vers le numérique n'est pas simplement une tendance : c'est une nécessité. La majorité des clients utilisent désormais les canaux en ligne et mobiles au quotidien. Les entreprises doivent donc proposer des services de haut niveau et des fonctionnalités optimales. En parallèle, ils doivent gérer la sécurité en ligne tout en proposant une expérience client fluide. C'est là qu'intervient la solution Kaspersky Fraud Prevention qui vous permet de développer vos canaux en ligne et mobiles sans vous soucier des problèmes de sécurité et d'accessibilité.

Kaspersky Fraud Prevention est alimenté par une gamme complexe de technologies avancées, notamment l'analyse comportementale et biométrique, l'analyse des appareils et de l'environnement. Le machine learning est appliqué pour la détection proactive des fraudes sophistiquées sur le Web et les canaux mobiles. Il permet aux systèmes de surveillance de la fraude de bénéficier d'un contexte supplémentaire pour une prise de décision plus précise et proactive, ainsi que de l'authentification à étapes intelligente et adaptative.

La solution se compose de deux produits complets qui peuvent être utilisés séparément, pour résoudre des problèmes commerciaux pertinents, ou ensemble, pour améliorer significativement les niveaux de sécurité et la protection contre la fraude ainsi que l'expérience de l'utilisateur.

L'authentification avancée a été développée pour améliorer l'expérience utilisateur, réduire le coût de l'authentification à deux facteurs et détecter en permanence les activités suspectes, pour obtenir des niveaux de sécurité plus élevés.

Dès la première connexion, l'authentification avancée analyse en permanence les événements, ce qui permet de calculer les niveaux de risque et de formuler des recommandations appropriées.



L'analyse automatisée des fraudes utilise une combinaison parfaitement équilibrée de technologies de pointe, de Threat Intelligence au niveau mondial et d'expertise humaine. Cette fonctionnalité permet d'identifier et d'alerter l'entreprise d'une éventuelle activité frauduleuse à l'avance, en analysant des données cruciales pour permettre de prendre des décisions précises et opportunes et de découvrir des cas de fraude complexes.

Les événements au cours des sessions utilisateurs qui affectent les utilisateurs, leurs appareils et leurs environnements alimentent les systèmes de gestion de la fraude avec les données nécessaires à une prise de décision rapide et précise. Les incidents prêts à l'emploi générés au sein de Kaspersky Fraud Prevention Cloud donnent un aperçu des cas réels de fraude et permettent d'aller directement au cœur du problème.

En plus des technologies performantes et de l'expertise, Kaspersky Fraud Prevention offre :

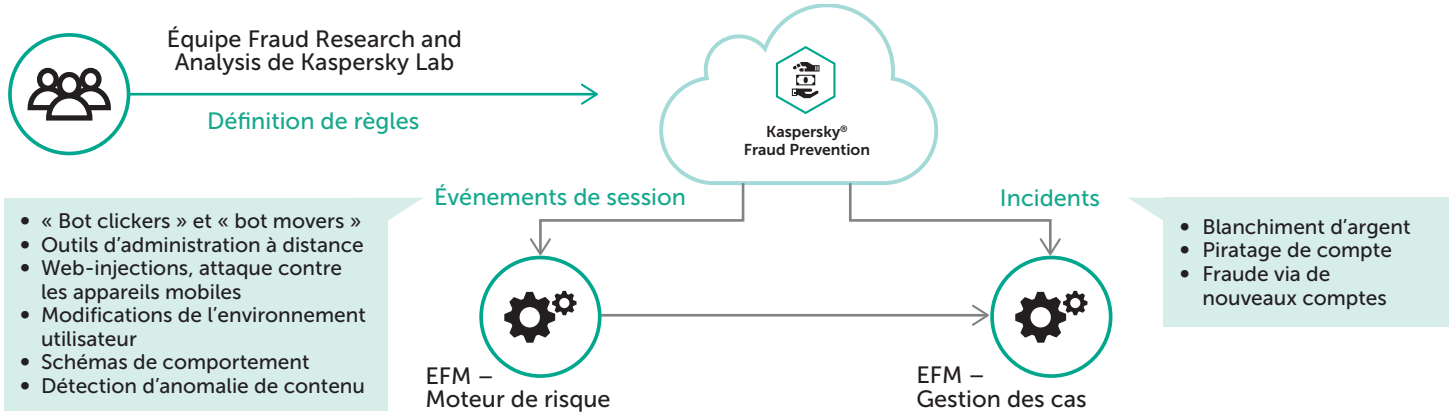
Accord de service de maintenance : une assistance améliorée pour tous vos besoins de sécurité, pour protéger votre entreprise avec l'assistance performantes de nos équipes locales d'ingénieurs certifiés.

Services de mise en œuvre : des ingénieurs de mise en œuvre spécialisés qui relient notre gamme de produits aux solutions existantes en matière de sécurité et de prévention de la fraude.

Conseil en prévention de la fraude : conseils aux entreprises pour aider à construire la bonne stratégie de prévention de la fraude prodigués par une équipe de professionnels avec un éventail de compétences d'experts et une expertise multi-industrielle.

Principaux avantages de Kaspersky Fraud Prevention :

- Croissance des systèmes en ligne et mobiles sans le stress supplémentaire des problèmes de sécurité et de convivialité
- Contrôle des coûts de prévention de la fraude et réduction des pertes dues à la fraude
- Détection en temps réel de la fraude avant qu'une transaction n'ait lieu
- Enrichir les solutions de surveillance de la fraude au sein des entreprises avec des données supplémentaires.



IoT Security

Justifier la confiance de vos clients en protégeant leur vie privée

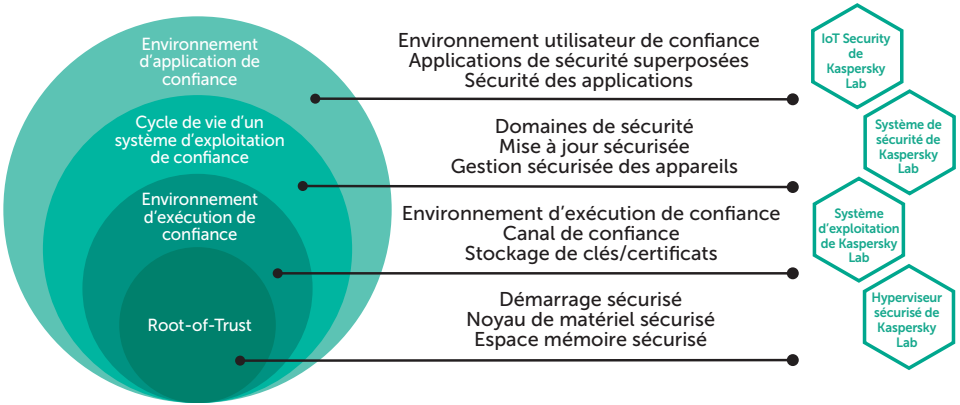
L'Internet des objets (IoT) est un nouveau paradigme qui change le monde. Il pourrait rendre notre monde plus sûr, améliorer notre santé, nous faire gagner du temps et de l'argent, réduire les déchets et ajouter une nouvelle dimension au contrôle de la production et à la vie en général.

La cybersécurité est traditionnellement associée à la sécurité des données personnelles. Cependant, à l'ère de l'IoT, elle concerne désormais la vie privée. Les violations de la vie privée des utilisateurs telles que la surveillance à distance par des caméras intelligentes, des moniteurs multimédias ou pour bébés, l'interférence dans le fonctionnement des appareils ménagers, les arrêts inattendus et la défaillance des services quotidiens, tout cela est inacceptable pour l'utilisateur final.

En même temps, l'Internet des objets offre d'énormes possibilités aux fabricants d'appareils (sans oublier les composants matériels et logiciels), aux fournisseurs de services de télécommunications et au marché de l'intégration de systèmes. Un manque de confiance dans les solutions d'IoT chez les utilisateurs finaux pourrait bloquer ou ralentir considérablement la réalisation de ces opportunités potentielles. C'est pourquoi la sécurité globale des solutions IoT est une priorité absolue pour toutes les personnes concernées...

En l'état actuel des choses, les appareils connectés et les équipements de télécommunications fournis aux clients peuvent facilement subir des violations de cybersécurité. Le matériel peut ne pas contrôler l'intégrité du micrologiciel et les appareils sont parfois livrés avec des mots de passe préinstallés, notamment les mots de passe administrateur. Des paramètres de sécurité réseau faibles ou l'utilisation de logiciels anciens et vulnérables peuvent également poser problème. Ajoutons à cela l'absence de processus de mise à jour logicielle, ce qui signifie que les appareils vulnérables peuvent fonctionner pendant des années sans mise à jour, il est donc clair que ce n'est qu'une question de temps avant que l'appareil ne soit attaqué.

Garanties de confiance au niveau de l'appareil



Le principe d'une chaîne de confiance constitue la base pour garantir le fonctionnement sûr d'un appareil connecté. Sans oublier les appareils et les éléments d'infrastructure (passerelles). Ce principe commence par l'utilisation d'une solution Root-of-Trust au niveau matériel.

Cette technologie effectue un démarrage fiable d'un système d'exploitation, dont la vérification de l'intégrité de l'image du système d'exploitation, l'application de la cryptographie et des mécanismes de stockage sécurisé assistés par du matériel pour les informations clés. Un démarrage fiable est crucial pour les appareils clés de l'infrastructure IoT tels que les passerelles, pour s'assurer que le système d'exploitation est démarré à partir de supports prédéfinis et seulement après que l'équipement a passé avec succès des vérifications d'intégrité spécifiques.

L'autre élément important de la chaîne de confiance est un système d'exploitation sécurisé capable d'assurer la bonne exécution d'un logiciel qui n'est pas considéré comme fiable. Les développements récents de la technologie informatique permettent de mettre en place un environnement au niveau du système d'exploitation qui restreint le comportement des applications qui ne peuvent pas être considérées comme fiables.

Le concept d'IoT englobe une grande variété d'appareils, de gadgets, de technologies, de logiciels et de protocoles de communication. Mais cet environnement hétérogène génère de nombreux risques de sécurité qui pourraient sérieusement entraver n'importe quel aspect de notre vie connecté à l'IoT. Kaspersky Lab a mis au point un certain nombre de produits qui permettent de minimiser les risques associés :

- **Embedded Systems Security**
  Renforcez et protégez vos appareils et ordinateurs embarqués basés sur Microsoft Windows avec une solution créée pour optimiser la sécurité des systèmes bas de gamme avec une capacité mémoire limitée, qui ne nécessite pas de maintenance continue ou de connectivité Internet.

- **KasperskyOS**
  Le système d'exploitation KasperskyOS est conçu pour protéger les systèmes embarqués divers et complexes contre les conséquences des codes malveillants, des virus et des attaques de pirates informatiques, grâce à une séparation forte et à l'application de règles. KasperskyOS crée un environnement où une vulnérabilité ou un mauvais code ne posent plus de problème. Le composant Kaspersky Security System contrôle les interactions sur l'ensemble du système, rendant l'exploitation des vulnérabilités inutile.

- **Kaspersky Security System**
  Kaspersky Security System est un moteur de calcul de diagnostic de politique de sécurité capable de travailler simultanément avec des types de politiques de sécurité différents (contrôle d'accès basé sur les rôles et obligatoire, logique temporelle, flux de contrôle, « type enforcement », etc.) et qui peut être personnalisé pour répondre aux besoins du client. Plus les règles sont précises, plus le contrôle et la sécurité de l'ensemble du système seront assurés.

  Kaspersky Security System peut être utilisé avec KasperskyOS (la configuration la plus sécurisée) ainsi que dans une solution basée sur Linux (actions sécurisées dans un système non sécurisé).

- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH) fonctionne sur le système à micronoyaux KasperskyOS. Avec KSH, les systèmes d'exploitation invités virtualisés potentiellement non fiables peuvent être séparés les uns des autres et toutes les communications entre eux peuvent être contrôlées et fiables, même s'ils fonctionnent physiquement sur la même plateforme matérielle. Un autre avantage de KSH est sa capacité à réduire les coûts de maintenance du matériel.

- **Kaspersky Transportation Security Service**
  Système « Security for Safety » intégré basé sur la technologie KasperskyOS : une passerelle sécurisée unique vers les unités de commande électronique (ECU) et une gamme de services d'évaluation de la sécurité répondant aux besoins des véhicules connectés actuels et futurs.

- **Unité de communication sécurisée**
  L'unité de communication sécurisée (SCU) est une unité de commande de passerelle de communication connectée à plusieurs sous-réseaux et/ou aux contrôleurs de passerelle de ces sous-réseaux dans le réseau automobile. Ainsi, la SCU est une passerelle unique vers les communications externes, alors que les appareils internes peuvent communiquer à l'intérieur d'un domaine ou même entre domaines sans utiliser les services de la SCU. La SCU est alimentée par KasperskyOS et renforcée par Kaspersky Security System. KasperskyOS contrôle toutes les interactions au sein de la SCU au niveau le plus bas et applique les résultats des politiques de Kaspersky Security System. Seules les interactions explicitement autorisées sont possibles.

Embedded Systems Security

Une solution de sécurité tout-en-un spécialement conçue pour les systèmes embarqués

Comme ils gèrent des opérations impliquant de l'argent réel et des informations d'identification de carte de crédit, les systèmes embarqués sont des cibles de choix pour les cybercriminels, et demandent donc les niveaux les plus élevés de protection. Il est temps maintenant d'appliquer des technologies éprouvées, telles que le contrôle des appareils et le blocage par défaut, en tant que première ligne de défense.

Aujourd'hui, les systèmes embarqués sont partout : dans les distributeurs de billeterie les DAB, les bornes, les systèmes de point de vente, les dispositifs médicaux, etc.

Les systèmes embarqués représentent une préoccupation particulière en matière de sécurité, en raison notamment de leur dispersion géographique, de la difficulté à les gérer et du manque de mises à jour. Les systèmes traitant des espèces et des identifiants doivent toutefois être résistants et tolérants aux pannes. Les systèmes embarqués ne doivent pas uniquement être protégés contre les menaces : les cybercriminels ou et autres cyberpirates ne doivent pas pouvoir s'en servir de point d'entrée pour pénétrer dans le réseau de l'entreprise.

La réglementation standard en matière de sécurité des systèmes embarqués a tendance à ne couvrir que la sécurité basée sur des antivirus ou le renforcement du système, ce qui n'est pas suffisant. Une approche purement antivirus est d'une efficacité limitée contre les menaces rencontrées actuellement par les systèmes embarqués, comme cela a été amplement démontré lors des dernières attaques.

Le blocage par défaut pour les applications, pilotes et bibliothèques, renforcé par une fonctionnalité de contrôle des appareils, est la seule approche capable d'assurer la sécurité de systèmes stratégiques obsolètes, mais toujours en usage.

La solution : Kaspersky Embedded Systems Security

Kaspersky Lab a conçu une solution de sécurité spécifiquement destinée aux entreprises gérant des systèmes embarqués. Cette solution reflète leurs fonctionnalités uniques, ainsi que leurs exigences en matière de système d'exploitation, de canal et d'équipement tout en se concentrant sur l'environnement de menaces spécifique auquel ces systèmes font face et en prenant totalement en charge la famille logicielle Windows XP.

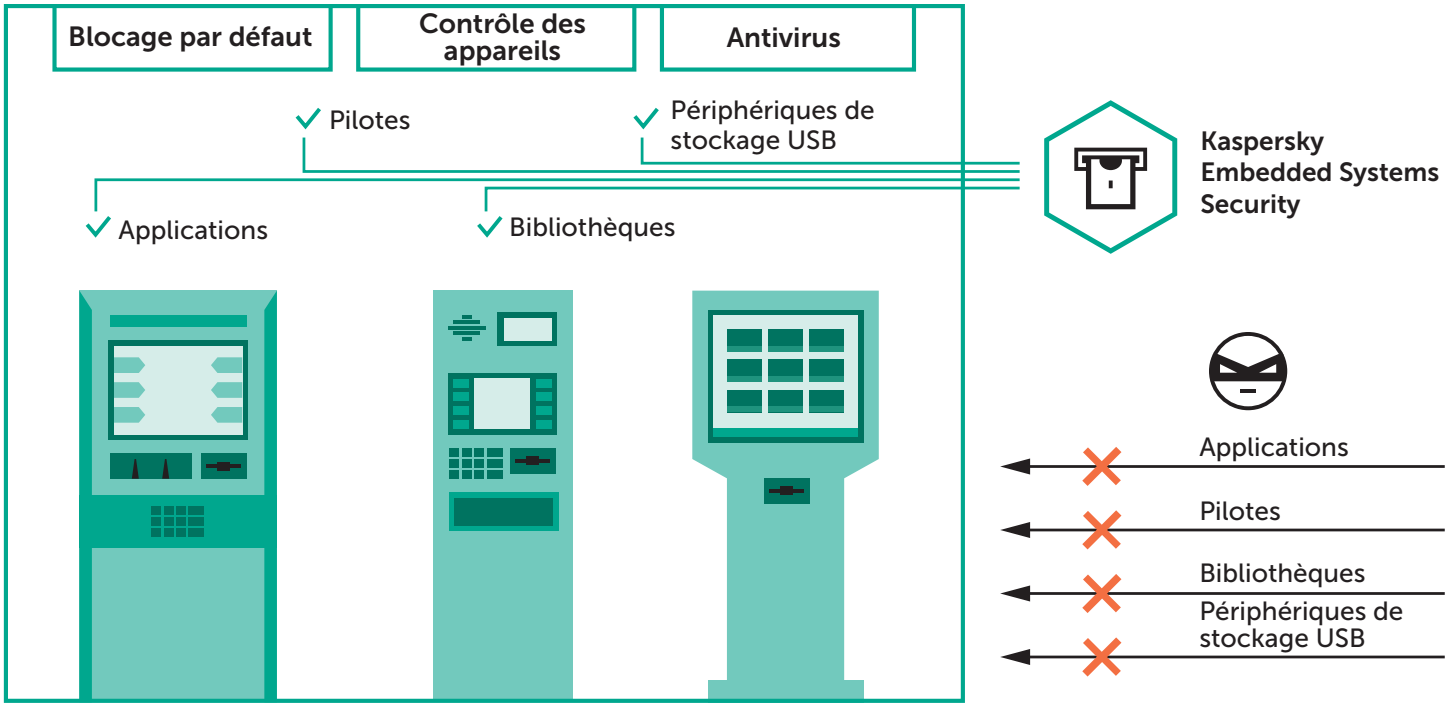
Kaspersky Embedded Systems Security propose un mode d'opération « blocage par défaut uniquement », où la configuration requise débute à 256 Mo de RAM et 50 Mo d'espace disque disponible, avec le système d'exploitation Windows XP et du matériel de faible puissance.

Un mode d'analyse à la demande assuré par un module antivirus livré en option est également disponible, gestion du pare-feu incluse. Ce module est alimenté par Kaspersky Security Network et assorti d'une fonctionnalité de gestion des correctifs, selon les besoins.

Cette solution unique répond donc à trois objectifs clés :

- Une sécurité efficace pour les systèmes « difficiles à gérer »
- Conformité avec les exigences PCI DSS 5.1, 5.1.1, 5.2, 5.3 et 6.2
- Un étalement chronologique en douceur pour le remplacement des systèmes et des équipements obsolètes.

La solution a été spécialement conçue pour réduire les risques de cybersécurité des infrastructures basées sur des systèmes d'exploitation embarqués, afin de protéger les surfaces d'attaque uniques à ces architectures, tout en respectant les équipements associés et les considérations en matière d'efficacité. Une console unique et intuitive vous donne le contrôle et la visibilité dont vous avez besoin pour gérer efficacement une sécurité multi-niveaux pour vos terminaux, vos systèmes clés et l'ensemble de votre infrastructure informatique.



Support premium et services professionnels

Une sélection de services afin de profiter au mieux des solutions Kaspersky Lab

Support premium

Lorsqu'un incident de sécurité se produit, le temps nécessaire à l'identification de sa cause et à son élimination est crucial. La détection et la résolution rapides d'un problème peuvent permettre aux entreprises de réaliser des centaines de milliers de dollars d'économie. Nos plans d'assistance Premium se concentrent précisément sur la réalisation de cet objectif. Accès 24 h/24 à nos experts, hiérarchisation appropriée et éclairée des problèmes avec des délais de réponse garantis et des correctifs privés : tout ce qui est nécessaire pour assurer la résolution de votre problème le plus vite possible.

Kaspersky Lab offre un choix de programmes d'assistance haut de gamme qui traitent vos problèmes de sécurité informatique comme une priorité absolue à tout moment, ce qui permet d'assurer le bon fonctionnement de votre entreprise, en concentrant toute notre expertise directement sur la recherche de la voie la plus rapide et la plus efficace pour vous ramener en toute sécurité à votre performance habituelle.

Nos offres de support premium comprennent :

- Responsable de compte technique (TAM)
- Support 24 h/24 et 7 j/7 via une ligne téléphonique dédiée
- Des accords de niveau de service pour les réponses aux incidents
- Des alertes proactives concernant les nouvelles menaces.

Services professionnels

La cybersécurité représente un investissement important. Faites appel à des experts qui comprennent exactement la façon dont vous pouvez optimiser vos investissements pour répondre aux besoins uniques de votre entreprise.

Nos experts en sécurité sont à votre disposition pour vous aider à déployer, configurer et mettre à niveau les solutions Kaspersky Lab sur toute l'infrastructure informatique de votre entreprise, dans le respect de notre méthodologie et des bonnes pratiques.

Les services professionnels de Kaspersky Lab s'assurent que votre réponse au changement ou votre transition est fluide, efficace et ne cause pas d'interruption indésirable des opérations commerciales.

Les services professionnels de Kaspersky Lab comprennent :

- Mise en œuvre et mise à niveau
- Configuration
- Health check
- Formation sur les produits.

À propos de Kaspersky Lab

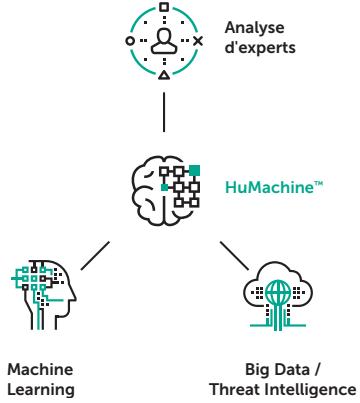
Kaspersky Lab est le plus important éditeur privé de solutions de sécurité informatique dans le monde. C'est aussi l'une des entreprises enregistrant la croissance la plus rapide du secteur.

Notre indépendance nous permet d'être plus flexibles, de penser différemment et d'agir plus rapidement. Nous innovons constamment, fournissons une protection efficace, adaptée et accessible. Nous sommes fiers de développer des systèmes de sécurité de renommée mondiale qui nous permettent, ainsi qu'à chacun de nos 400 millions d'utilisateurs et nos 270 000 clients professionnels, de conserver une longueur d'avance sur les menaces potentielles.

Notre engagement en faveur des personnes et nos technologies avancées nous distinguent également de la concurrence.

Rendez-vous sur www.kaspersky.fr/enterprise-security pour en savoir plus sur l'expertise unique de Kaspersky Lab et sur ses solutions de sécurité destinées aux entreprises.

Notes



Solutions de sécurité 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

© 2018 AO Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.