KASPERSKY lab

Kaspersky Enterprise Cybersecurity
#TrueCybersecurity

Solutions de sécurité Kaspersky Lab destinées aux entreprises

2017

Sécurisation des entreprises

Les cybermenaces sont de jour en jour plus sophistiquées. Sans solution efficace permettant de les atténuer, les entreprises sont à la merci de cyberattaques susceptibles d'impacter les ressources financières, de perturber la continuité des activités, d'exposer des données confidentielles, mais aussi de nuire à leur réputation. Une attaque réussie est extrêmement préjudiciable pour toute entreprise, indépendamment de son secteur d'activité.

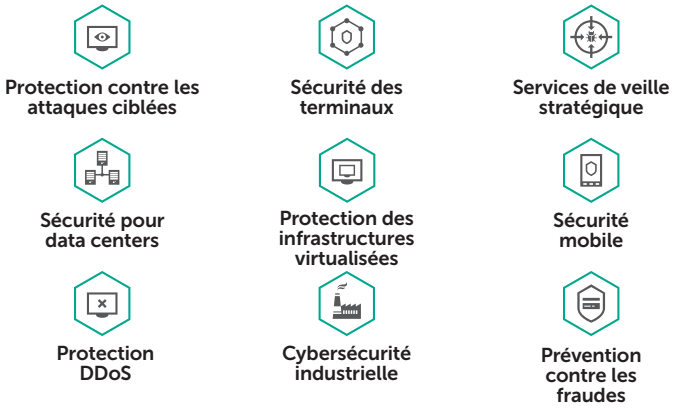
PRENDRE AU SÉRIEUX LA SÉCURITÉ DE L'ENTREPRISE

Les coûts liés à une défaillance au niveau de la sécurité sont élevés : dans l'enquête 2015 sur les risques informatiques mondiaux de Kaspersky Lab, nous avons constaté que le coût direct moyen de récupération pour une entreprise s'élève à 551 000 USD, en plus des coûts indirects atteignant en moyenne 69 000 USD. Afin d'éviter ces coûts et les perturbations qui y sont liées, les entreprises doivent renforcer le type et le niveau de protection au sein de leur infrastructure informatique.

Basées sur la veille stratégique qui forme le cœur de nos produits et de nos services, les solutions Kaspersky Lab offrent des fonctionnalités de prévision, de prévention, de détection et d'intervention pour de nombreux segments d'infrastructure et de technologies émergentes : terminaux, services en ligne et mobiles, infrastructures virtuelles, data centers, systèmes de contrôle industriel, etc.

Kaspersky Lab est l'un des premiers éditeurs à aider les entreprises à adapter leurs stratégies de sécurité afin de contrer encore mieux les toutes dernières menaces et les attaques ciblées. Nous proposons une combinaison unique de technologies et de solutions, soutenues par l'un des meilleurs services de veille stratégique au monde, afin d'aider les entreprises à détecter les attaques ciblées et à atténuer les risques à un stade précoce, avant que des dommages graves ne soient causés.

En couvrant tous les cas de figure possibles des incidents informatiques, les solutions Kaspersky Lab proposent une approche globale, évolutive et stratégique de la sécurité de l'entreprise. Notre philosophie est simple : garantir une protection optimale à partir d'une expertise supérieure combinée à une technologie de pointe.



Anti Targeted Attack

Une solution reposant sur la veille stratégique des attaques ciblées

Les attaques ciblées sont des processus à long terme qui compromettent la sécurité et permettent au cybercriminel d'obtenir le contrôle des outils informatiques de sa victime, tout en évitant d'être repéré par les technologies de sécurité traditionnelles.

Tandis que certains cybercriminels utilisent des menaces persistantes avancées (APT), qui peuvent être très efficaces mais très coûteuses à mettre en œuvre, d'autres font appel à des « attaques ciblées » bien moins chères à élaborer, mais qui peuvent s'avérer tout aussi dévastatrices. Reposant sur des techniques de base (ingénierie sociale, usurpation de données d'identification d'employés, logiciels d'apparence authentiques ou programmes malveillants couverts par un certificat volé), ces attaques ciblées peuvent ne pas faire les gros titres, mais elles sévissent partout dans le monde.

La plupart des grandes entreprises ont déjà considérablement investi dans des solutions de sécurité informatique traditionnelles, surtout au niveau de la passerelle. Cependant, même si ces technologies de sécurité préventive peuvent s'avérer très efficaces pour se protéger contre les menaces les plus courantes (notamment les programmes malveillants, les fuites de données, les attaques réseau, etc.), elles ne sont manifestement pas suffisantes : le nombre total d'incidents et d'atteintes à la sécurité des entreprises n'a pas baissé d'un iota.

À l'heure actuelle, même avec des technologies innovantes telles que Sandbox, EDR et autres solutions « nouvelle génération », la problématique est la même : comment mettre le doigt sur le bon incident et déterminer l'incident associé aux menaces les plus importantes. Les solutions de détection spécialisées jouent un rôle essentiel dans l'identification des incidents qui méritent une investigation et une intervention plus poussées.

Les menaces avancées et ciblées peuvent agir sans être détectées pendant 200 jours voire plus, tandis que les cybercriminels rassemblent discrètement de précieuses informations et/ou perturbent des processus métiers essentiels.

Selon les statistiques de Kaspersky Lab, un seul incident par attaque ciblée peut coûter plus de 2,5 millions de dollars à une entreprise, un montant disproportionné par rapport au capital de départ d'une PME qui s'élève en moyenne à 80 000 USD.

Sans intervention, une attaque ciblée a toutes les chances de provoquer de sérieux dommages à l'entreprise, et notamment les suivantes :

- pertes financières considérables
- perte de données sensibles
- contrôle à distance par le cybercriminel de processus métiers apparemment « autorisés »
- manipulation discrète de données

Dans une étude sur les grandes entreprises menée par Kaspersky Lab en 2015, 1 entreprise sur 4 (soit 23 %) a confirmé avoir déjà fait l'objet d'au moins une attaque ciblée.

SOLUTION : LA PLATE-FORME KASPERSKY ANTI TARGETED ATTACK

La plate-forme Kaspersky Anti Targeted Attack fait partie d'une approche adaptable et intégrée de la sécurité de l'entreprise. La surveillance du trafic réseau, associée au sandboxing d'objet et à l'analyse du comportement des terminaux, fournit un aperçu détaillé de ce qui se passe précisément dans toute l'infrastructure informatique d'une entreprise. Cette approche adaptable de la sécurité protège les entreprises contre la plupart des menaces sophistiquées, des attaques ciblées, des nouveaux programmes malveillants, notamment les programmes ransomware et crimeware, et bien sûr contre les menaces persistantes avancées.

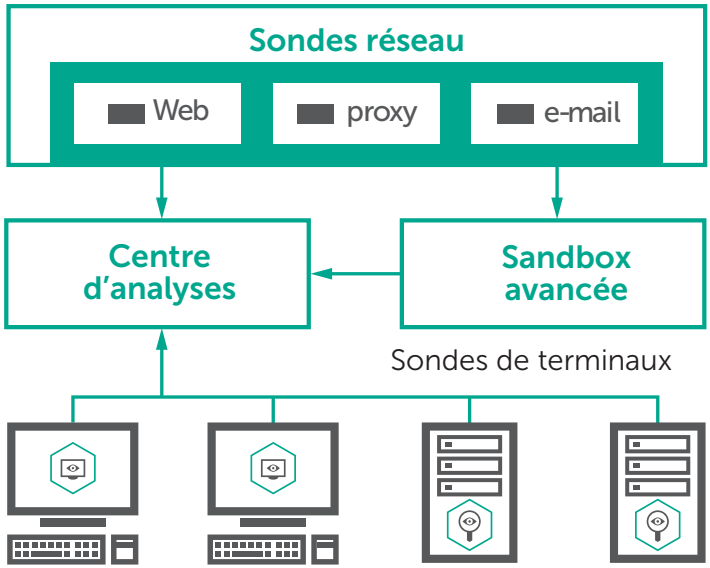
En mettant en corrélation des événements issus de plusieurs niveaux, y compris le réseau, les terminaux et le paysage mondial de menaces, la plate-forme Kaspersky Anti Targeted Attack fournit une détection « quasiment en temps réel » des menaces complexes tout en générant des données d'analyses criminalistiques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

Notre service de veille stratégique mondiale leader du secteur est l'une des raisons qui nous permet d'atteindre ces performances de détection supérieures. Aucun autre fournisseur de sécurité ne peut égaler la qualité et l'ampleur de notre service de veille stratégique, qui nous permet de protéger les entreprises contre un éventail de menaces toujours croissant.

Par ailleurs, le service de veille stratégique mondiale n'est que le début : la plate-forme Kaspersky Anti Targeted Attack incorpore également plusieurs puissantes technologies de détection et d'analyse, comprenant :

- **une architecture de sondes multi-niveaux**, pour une visibilité à 360 degrés. Grâce à une combinaison de sondes réseau, Web et de messagerie électronique, ainsi que de sondes de terminaux, la plate-forme Kaspersky Anti Targeted Attack offre une détection avancée à chaque niveau de votre infrastructure informatique d'entreprise.
- **une sandbox avancée :** pour évaluer les nouvelles menaces. Issue d'une élaboration continue de plus de 10 ans, notre sandbox avancée offre un environnement isolé et virtuel où les objets suspects peuvent être exécutés en toute sécurité, afin d'en observer le comportement.
- **des moteurs d'analyse puissants**, pour des diagnostics rapides et moins de faux positifs. Notre analyseur d'attaques ciblées évalue les données du réseau et des terminaux saisies par les sondes, puis génère rapidement des diagnostics de détection des menaces destinés à l'intention de votre équipe de sécurité.

Plate-forme Kaspersky Anti Targeted Attack



Kaspersky Private Security Network

Tous les avantages d'une surveillance des menaces dans le Cloud au sein de votre infrastructure

Les solutions de sécurité standard ont besoin de quatre heures pour recevoir les informations nécessaires à la détection et à l'interception des quelque 310 000 nouveaux programmes malveillants découverts chaque jour par les chercheurs de Kaspersky Lab. Le service de partage des informations sur les menaces via le réseau Kaspersky Private Security Network fournit ces données en 30 à 40 secondes.

La cybercriminalité évolue, non seulement en termes d'ampleur, mais aussi de sophistication ; bien que 70 % des menaces auxquelles sont confrontées quotidiennement les entreprises soient connues, 30 % restent des menaces inconnues et avancées que les solutions de sécurité traditionnelles basées sur les signatures sont bien incapables de gérer seules.

Kaspersky Security Network offre à chaque système connecté à Internet les informations de sécurité recueillies par Kaspersky Lab, ce qui permet de garantir un délai d'intervention très rapide, un taux de faux positifs moins élevé et un niveau de protection optimal, y compris contre les menaces inconnues et avancées.

Bien que les informations traitées par Kaspersky Security Network soient totalement anonymes et dissociées de leur source, nous savons que certaines entreprises exigent un verrouillage absolu des données. Avant, cela signifiait que ces entreprises ne pouvaient pas tirer parti des solutions de sécurité basées dans le Cloud.

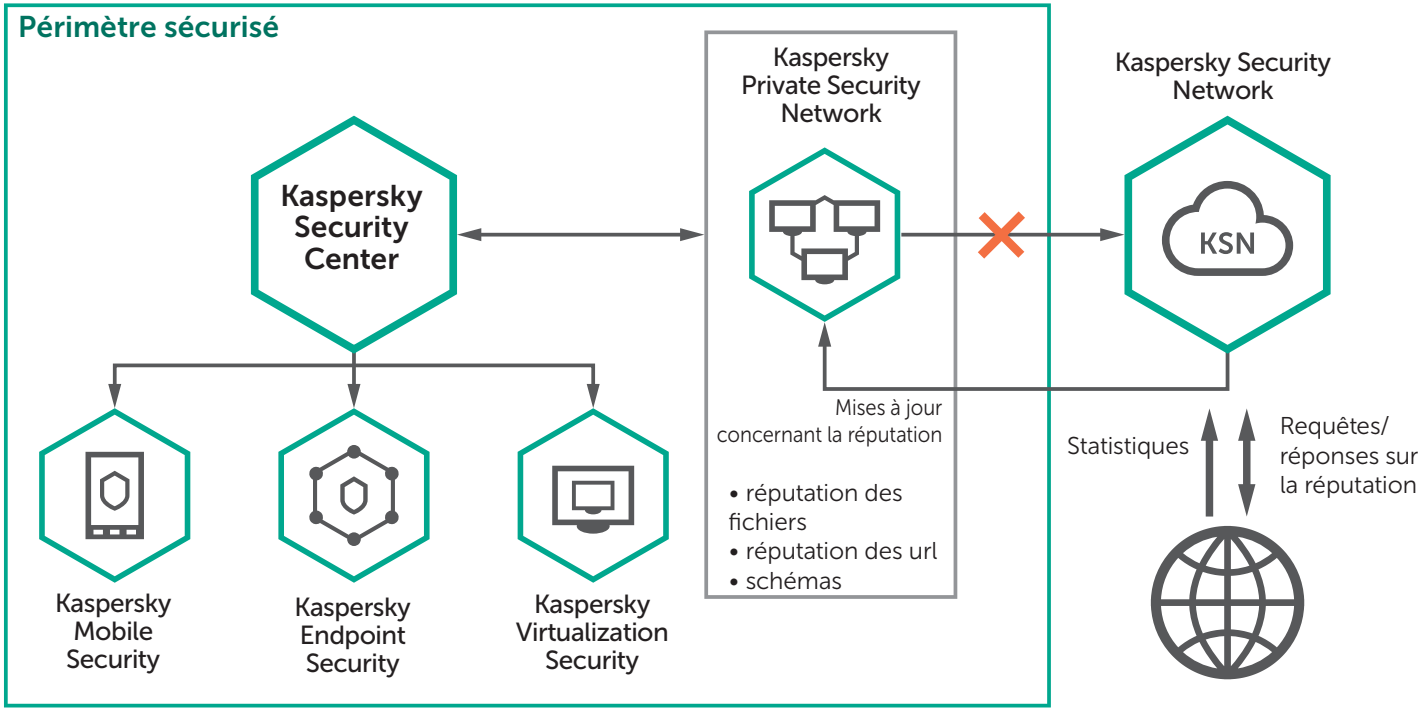
LA SOLUTION : KASPERSKY PRIVATE SECURITY NETWORK

Pour les clients avec ces besoins spécifiques, Kaspersky Lab a développé Kaspersky Private Security Network, qui permet aux entreprises de bénéficier de la plupart des avantages liés à la sécurité assistée par le Cloud sans diffuser de données hors de leur périmètre de contrôle. 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 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).
- Réduit les faux positifs.
- Respecte les normes strictes en matière de confidentialité, de sécurité et de réglementation.

Kaspersky Private Security Network n'applique pas uniquement nos informations et renseignements uniques sur les menaces aux solutions de sécurité de Kaspersky Lab, mais également aux autres solutions que l'entreprise utilise, notamment les solutions de SIEM, de gestion des risques et de conformité. Toutes ces fonctionnalités peuvent être intégrées via SDK, appels directs et l'API de Kaspersky Private Security Network, offrant ainsi une visibilité unique sur la sécurité et les capacités de défense de votre entreprise.



Endpoint Security

Protection multi-niveaux nouvelle génération contre les menaces sophistiquées les plus récentes visant vos terminaux

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.

Avec le développement de l'activité numérique, les environnements informatiques d'entreprise sont devenus encore plus complexes. En parallèle, les cybercriminels développent des techniques d'attaque de plus en plus sophistiquées, créant de nouveaux moyens d'infiltrer les infrastructures d'entreprise.

La majorité des cyberattaques qui touchent les entreprises sont lancées via les terminaux. Sans apprentissage automatique ni veille stratégique mondiale efficace, les technologies de protection traditionnelles ne sont pas en mesure de vous protéger contre les menaces hautement sophistiquées.

Nous offrons une protection instantanée contre les menaces avancées et inconnues et les attaques ciblées grâce à nos technologies de détection avancée, qui s'appuient sur l'apprentissage automatique et la veille stratégique.

La protection contre les menaces avancées est encore améliorée grâce à des outils puissants de protection des données et de contrôle (par exemple, le chiffrement intégré, l'application automatique de correctifs et la protection des terminaux mobiles), qui sont tous gérés via Kaspersky Security Center.

Tous les composants sont développés en interne et constituent une plate-forme commune facilement adaptable pour répondre à l'évolution des besoins de l'entreprise.

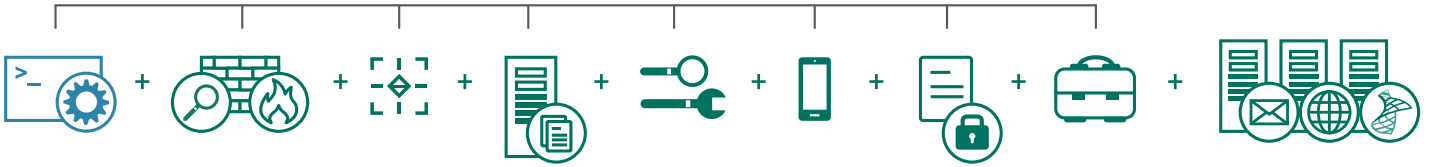
LA SOLUTION : KASPERSKY ENDPOINT SECURITY

La sécurisation totale de chaque terminal contre toute forme de cybermenace avancée est essentielle. La protection antivirus traditionnelle n'est en aucun cas suffisante. Ce n'est qu'en employant une plate-forme de sécurité de pointe incluant l'apprentissage automatique pour une détection statique et dynamique et en adoptant une approche multi-niveaux que vous pouvez espérer protéger totalement chaque terminal, dans et au-delà de votre périmètre.

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

Il n'existe pas de meilleur choix en matière de sécurité pour votre entreprise.

Kaspersky Endpoint Security



Protection éprouvée sans précédent de tous les types de terminaux
Nos technologies de protection avancée sécurisent les grandes entreprises et leurs infrastructures informatiques, quelle qu'en soit la complexité, y compris chaque terminal, des serveurs et des bureaux virtuels et physiques aux appareils mobiles.

Analyse de comportement utilisant l'apprentissage automatique pour protéger votre entreprise
Nos solutions utilisent l'apprentissage automatique basé sur des technologies de données dynamiques et statiques. Grâce à cela, nous sommes même capables de vous protéger contre les menaces futures.

Veille stratégique mondiale de haut niveau
Toutes nos technologies sont basées sur notre veille stratégique mondiale éprouvée. Nous avons découvert plus de menaces APT que tout autre fournisseur de solutions de sécurité. De ce fait, nous disposons d'une connaissance inégalée de la nature des menaces modernes, et pouvons vous aider à mieux vous protéger contre ces dernières.

Réponse automatique en temps réel
Dès qu'une menace est détectée, le système annule toutes les modifications détectées par notre moteur de surveillance dynamique des comportements que le programme malveillant a déjà lancées.

Protection dynamique continue contre les vulnérabilités et les menaces de type « zero-day »
La protection automatique contre les failles d'exploitation a été développée afin d'empêcher les cybercriminels de cibler les vulnérabilités des applications installées sur des machines protégées. La gestion automatique des correctifs offre un niveau de sécurité renforcé.

Protection des données certifiée FIPS 140-2
Le chiffrement puissant et transparent vis-à-vis des utilisateurs sécurise totalement les données sensibles sur les mobiles, les appareils portables et fixes.

Protection de haut niveau contre les ransomwares
Sécurisez vos données, empêchez les cybercriminels de gagner de l'argent au moyen de rançons, et protégez les dossiers partagés contre les cryptovirus grâce à nos technologies de protection contre les ransomwares.

Un coût total de possession (TCO) plus faible et un retour sur investissement (ROI) plus élevé grâce à la gestion centralisée et unifiée
Gérez plusieurs plates-formes et l'ensemble des terminaux à partir d'une seule et même console, et gagnez en visibilité et en contrôle sans investissement supplémentaire en termes de logiciels, d'équipement ou de ressources humaines.

Embedded Systems Security

Protection puissante conçue spécialement 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 intelligente dédiée. 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 automatiques de billets de toutes sortes, 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 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.

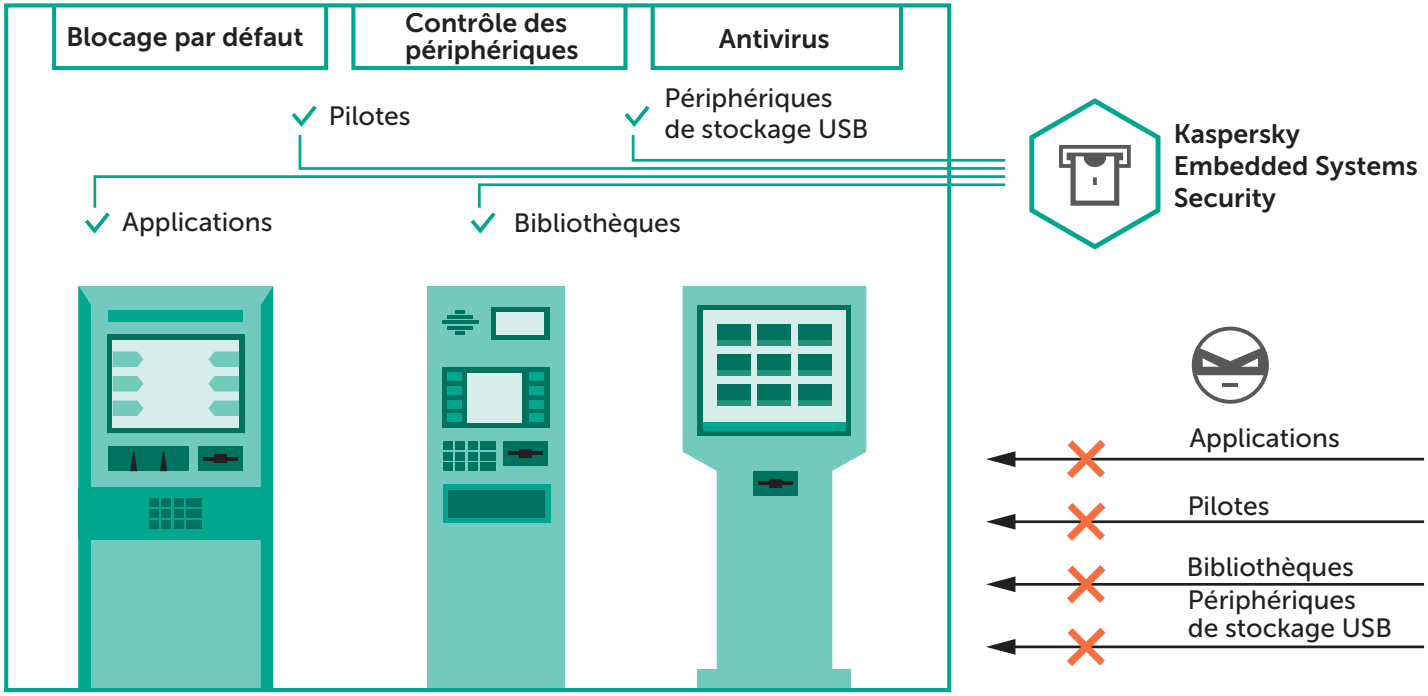
Kaspersky Embedded Systems Security propose un mode d'opération « blocage par défaut uniquement », où la configuration requise débute à 256 Mo de RAM et 50 Mo d'espace disque disponible, avec le système d'exploitation Windows XP et du matériel de faible puissance.

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 »
- La 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.



Services de veille stratégique

Veille stratégique de premier plan, services spécialisés et formation à la sécurité

60 % des grandes entreprises prévoient d'utiliser des services de surveillance des menaces dans le cadre de leur stratégie de sécurité.

De nouvelles menaces sophistiquées apparaissent constamment, tandis que les cybercriminels développent des techniques innovantes capables de déjouer les technologies de sécurité établies. Les solutions de sécurité traditionnelles telles que les antivirus, les pare-feu et les systèmes de prévention contre les intrusions ne suffisent plus à garantir une protection complète. Aujourd'hui, une nouvelle approche de la sécurité, basée sur une expertise étendue et des informations exhaustives sur les menaces, est nécessaire pour combler ce vide en matière de sécurité.

En partageant ses informations les plus récentes avec ses clients, Kaspersky Lab aide les entreprises à se protéger de ces menaces. Notre vaste gamme de services de veille stratégique permet à votre centre des opérations de sécurité (SOC) et/ou équipe de sécurité informatique de protéger l'entreprise contre les toutes dernières menaces en ligne.

FORMATION À LA CYBERSÉCURITÉ

La sensibilisation et la formation à la cybersécurité sont des impératifs pour les entreprises confrontées à un volume croissant de menaces en constante évolution.

Vos spécialistes internes chargés de la sécurité doivent bien maîtriser les techniques de sécurité avancées, qui constituent l'un des éléments clés d'une stratégie efficace de gestion et de réduction des menaces en entreprise. Par ailleurs, tous les employés doivent être sensibilisés aux dangers et aux méthodes de travail sécurisées.

Nous proposons un large choix de programmes de formations :

- **La sensibilisation à la cybersécurité** permet aux entreprises d'améliorer les compétences de leurs employés en matière de sécurité et, par conséquent, la sécurité de l'entreprise elle-même.
- **Formation à la sécurité pour les professionnels de la sécurité informatique** : couvrant tous les niveaux (du niveau de base au niveau expert en analyse de programmes malveillants), elle améliore les compétences des experts en sécurité de votre entreprise et réduit les risques d'incidents.

SURVEILLANCE DES MENACES

Votre système SIEM dispose-t-il des capacités nécessaires de détection des cybermenaces ? Pouvez-vous avoir l'assurance d'être averti à temps des menaces les plus dangereuses ? Notre portefeuille de services de surveillance des menaces est conçu pour donner aux entreprises les outils nécessaires pour gérer ces risques :

- **Flux d'informations sur les menaces :** optimisez votre solution SIEM et approfondissez vos compétences en matière de criminalité grâce à nos toutes dernières informations sur les cybermenaces.
- **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).
- **Les rapports de veille sur les menaces spécifiques au client** identifient toutes les composantes essentielles de votre réseau disponibles à l'extérieur.

SERVICES D'EXPERTS

Votre expertise interne est-elle suffisante pour résoudre un cyberincident ? Votre infrastructure informatique et vos applications spécifiques sont-elles entièrement sécurisées face aux cyberattaques potentielles ? Nos services d'experts sont conçus pour atténuer et résoudre ces risques :

- **Tests de pénétration :** apprenez à identifier les points les plus faibles de votre infrastructure et à éviter les dommages provoqués par les cyberattaques. Respectez ainsi les normes du gouvernement, du secteur et de l'entreprise (par ex. PCI DSS).
- **Évaluation de la sécurité des applications** : ce service permet d'identifier les vulnérabilités des applications, des solutions basées dans le Cloud, systèmes ERP, services bancaires en ligne et autres applications professionnelles spécialisées aux applications mobiles et embarquées sur différentes plates-formes.
- **Cyberdiagnostic et analyse des programmes malveillants :** ce service retrace de façon détaillée l'historique de tout incident à partir de rapports complets, comprenant notamment les différentes étapes de résolution de l'incident.

Sensibilisation à la cybersécurité

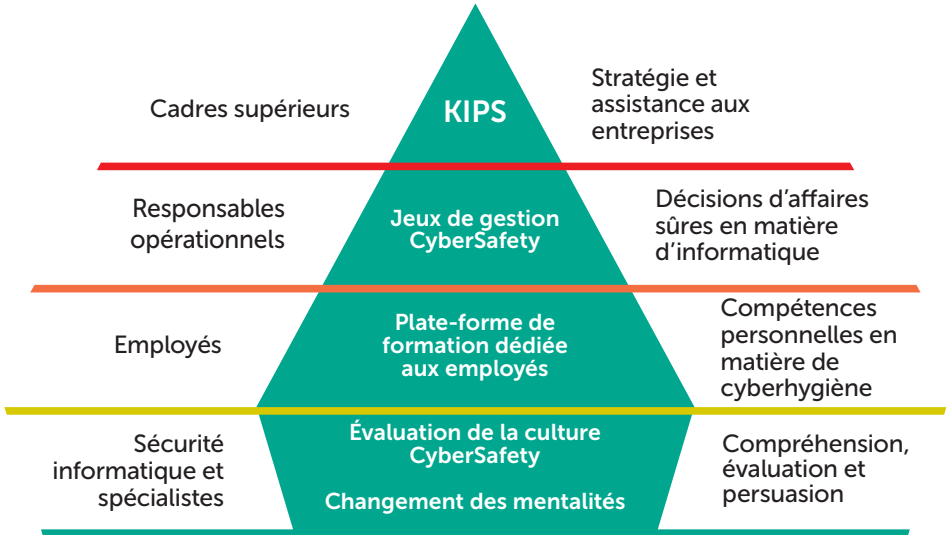
Créer un environnement informatique sécurisé grâce à la formation

Plus de 80 % des incidents informatiques sont dus à l'erreur humaine. En moyenne, les grandes entreprises dépensent 551 000 $ pour se remettre d'une faille de sécurité, tandis que ce montant s'élève à 38 000 $ pour les PME. À elles seules, les attaques de phishing coûtent jusqu'à 400 $ par employé 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 a lancé une gamme de formations 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 Kaspersky Lab :

- 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

L'APPROCHE KASPERSKY LAB

- **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.
- **Évaluation en temps réel, gestion du programme sans effort** : la plate-forme de formation en ligne 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 aux 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).

DESCRIPTION

- La formation aborde un large éventail de questions de sécurité : fuite de données, ransomware, 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 employés, 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 de sécurité informatique du client de tirer le meilleur parti des initiatives de sensibilisation à la sécurité.

Security For Data Centers

Un équilibre parfait entre protection et performances pour les data centers hybrides

Les data centers définis par logiciel requièrent la même protection que leurs homologues traditionnels. Si vous ne respectez pas cette exigence, vos systèmes virtualisés et volumes de stockage de données deviennent alors le maillon le plus faible de la chaîne de sécurité de votre data center.

Les grandes entreprises traitent des volumes de données de plus en plus importants. Afin de suivre ce rythme, les entreprises doivent repenser non seulement leurs méthodes de stockage et d'accès aux données, mais aussi la manière dont elles préservent leur sécurité et leur intégrité. Plus l'infrastructure est étendue, plus la quantité de données d'entreprise sensibles conservées est importante et plus les exigences porteront sur la puissance et la fiabilité de la solution de sécurité qui les protège.

Que vous gériez votre propre data center ou que vous utilisiez les services d'un tiers (par le biais d'une infrastructure en tant que service ou IaaS), votre solution de sécurité ne doit pas uniquement protéger efficacement et continuellement l'ensemble des données vitales : elle doit également préserver les performances de l'infrastructure du data center.

Tout data center offre de nombreuses surfaces d'attaque vulnérables à une exploitation potentielle. À mesure que votre data center s'étendra il sera également voué à évoluer en complexité, ce qui offrira d'autant plus d'occasions à la communauté des cybercriminels. Votre solution de sécurité doit être prête à relever le défi et à s'adapter en conséquence, en s'intégrant totalement à votre infrastructure informatique existante. Dans le cas contraire, elle réduira le niveau de performances de votre data center et affaiblira votre efficacité opérationnelle globale au fur et à mesure de votre croissance.

LA SOLUTION : KASPERSKY SECURITY FOR DATA CENTERS

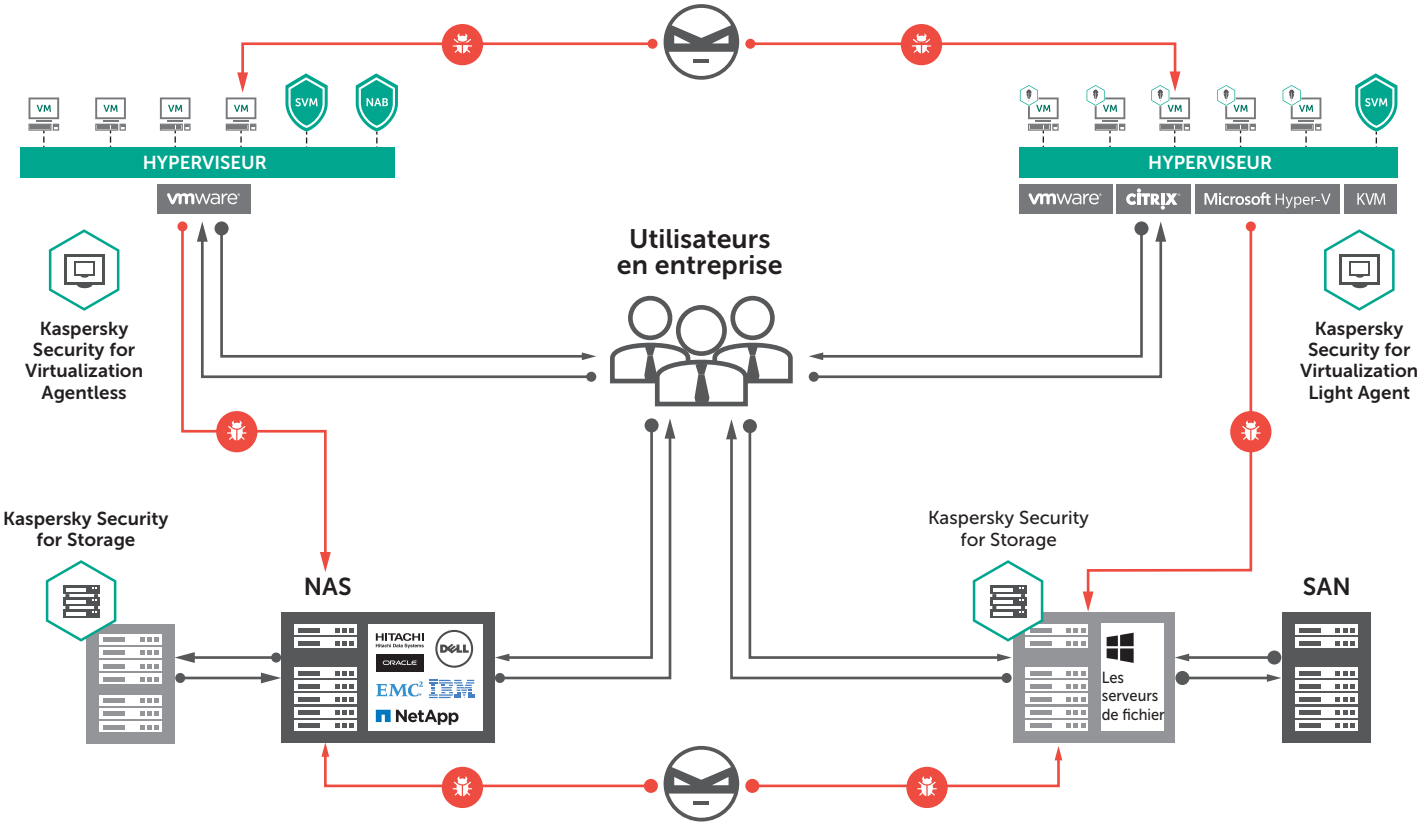
Nous proposons des solutions centrées sur la protection de deux secteurs essentiels de votre data center : l'infrastructure virtuelle et les systèmes de stockage de données. Idéale pour les environnements à plusieurs hyperviseurs et systèmes de stockage, la solution de Kaspersky Lab comprend :

- des mesures de sécurité conçues spécifiquement pour les plates-formes principales de virtualisation, dont VMware avec NSX, Citrix, Microsoft et KVM.
- des mesures de sécurité destinées aux systèmes de stockage en réseau (NAS), notamment EMC, NetApp, DELL, IBM, Hitachi et Oracle.

Kaspersky Security for Data Centers repose sur notre moteur de sécurité maintes fois primé et opère en tant que plate-forme intégrée unique, facilitant ainsi sa gestion et son intégration à différentes configurations de data centers. L'administration centralisée signifie que votre équipe peut appliquer des politiques de sécurité unifiées à l'ensemble de votre data center, ce qui permet ainsi de réduire les coûts de fonctionnement.

Cette solution complète :

- protège vos données et vos systèmes des cyberattaques
- fournit des outils efficaces pour garantir des niveaux élevés de performance et de continuité de l'activité
- permet à votre équipe de gérer la sécurité de toutes les machines, virtuelles et physiques, du data center depuis une console centralisée unique


VM
SVM
NAB
HYPERVISEUR
vmware
Kaspersky Security for Virtualization Agentless
Utilisateurs en entreprise
CITRIX
Microsoft Hyper-V
KVM
Kaspersky Security for Virtualization Light Agent
Kaspersky Security for Storage
NAS
HITACHI
ORACLE
DELL
EMC²
IBM
NetApp
Les serveurs de fichier
SAN

Security for Virtualization

Protection supérieure, souple et efficace pour les serveurs virtuels et les environnements VDI

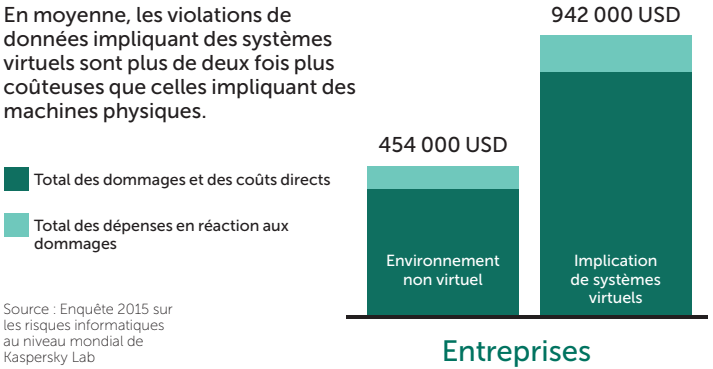
En matière de sécurité des systèmes virtuels, les entreprises cherchent le bon équilibre entre protection et performance, ainsi que les fonctionnalités de sécurité les plus avancées afin de maintenir la sécurité de leurs processus métiers stratégiques.

Alors que les entreprises continuent à déployer des environnements virtualisés sur une part de plus en plus importante de leur parc informatique, un besoin croissant de sécurité conçue spécifiquement pour la virtualisation se fait sentir. Or, il est difficile de trouver une solution qui offre des fonctionnalités de protection aussi bien pour les infrastructures de bureaux virtuels (VDI) en pleine croissance que pour votre environnement de serveurs virtuels, tout en conservant les avantages de la virtualisation en termes de performance. Malgré tous ses avantages, la virtualisation crée également un certain nombre de « surfaces d'attaque » supplémentaires et offre aux cybercriminels encore plus d'occasions de s'en prendre aux très grandes entreprises.

La solution sécurisant votre infrastructure virtualisée doit garantir une protection continue et offrir des fonctionnalités étendues tout en préservant l'efficacité de votre infrastructure virtuelle.

L'architecture unique de la solution spécialisée conçue par Kaspersky Lab fournit une protection multi-niveaux efficace pour les machines virtuelles (VM) sans sacrifier les performances. Résultat : les ratios de consolidation sont bien plus élevés qu'avec les solutions de lutte contre les programmes malveillants traditionnelles. Les « blitz de mise à jour » et les « blitz antivirus » sont désormais éliminés, ainsi que les fenêtres de vulnérabilité ou les « clichés instantanés ». Avec ses couches de protection supplémentaires combinées à des mécanismes de prévention des intrusions sur le réseau, la solution de Kaspersky Lab fait franchir un nouveau palier à la sécurité des plates-formes de virtualisation des entreprises.

En moyenne, les violations de données impliquant des systèmes virtuels sont plus de deux fois plus coûteuses que celles impliquant des machines physiques.



Source : Enquête 2015 sur les risques informatiques au niveau mondial de Kaspersky Lab

Pour une grande entreprise, le coût moyen de récupération après une violation de la sécurité virtuelle s'élève à plus de 940 000 USD, soit deux fois plus qu'un incident comparable n'impliquant que l'infrastructure physique.

Si une attaque sur nœuds physiques conduit à une incapacité temporaire d'accéder aux informations essentielles à l'activité dans 36 % des incidents signalés, ce pourcentage passe à 66 % lorsque l'attaque affecte des serveurs et des bureaux virtuels.

LA SOLUTION : KASPERSKY SECURITY FOR VIRTUALIZATION

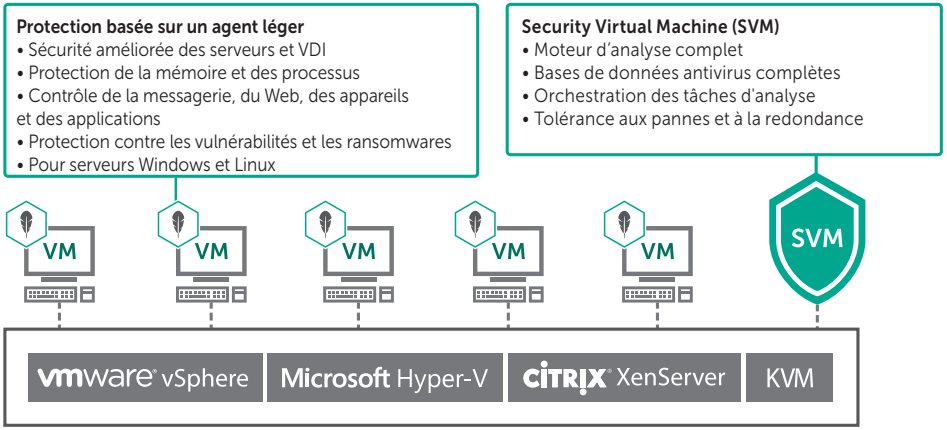
Kaspersky Lab propose deux technologies vous permettant d'atteindre cet équilibre parfait entre une sécurité optimale et des performances préservées.

Tandis que notre solution sans agent fonctionne en collaboration avec les technologies hyperviseur essentielles (par exemple VMware NSX), notre solution avec agent léger propose des couches de protection supplémentaires pour chaque machine virtuelle.

Afin de protéger leurs machines virtuelles, les entreprises n'ont besoin de déployer qu'une seule machine virtuelle de sécurité (SVM), à laquelle les tâches d'analyse au niveau des fichiers peuvent être confiées. Cette SVM fournit une protection centralisée contre les programmes malveillants à toutes les machines virtuelles de l'hôte sans consommation de ressources supplémentaires. Des technologies intégrées de tolérance aux pannes et de redondances confèrent à votre solution de sécurité la fiabilité dont vous avez besoin pour assurer avec succès vos opérations commerciales.

Déployer un agent léger sur chaque machine virtuelle ajoutera à l'ensemble une protection multi-niveaux et des contrôles de sécurité dotés de nombreuses fonctionnalités. La sécurité de vos machines virtuelles, qu'elle soit sans agent, basée sur un agent léger ou les deux, peut être gérée depuis une console unique, de même que celle de vos terminaux et serveurs physiques et celle de vos appareils mobiles.

Technologie unique avec agent léger de Kaspersky Lab



Kaspersky Security for Virtualization s'intègre étroitement à la plupart des plates-formes de virtualisation les plus répandues : VMware vSphere avec NSX, KVM, Microsoft Hyper-V et Citrix XenServer. Notre solution de sécurité est optimisée pour sauvegarder les performances de votre plate-forme en tirant pleinement parti des propres technologies de base de votre hyperviseur, en complétant et en renforçant la sécurité de VMware Horizon et Citrix XenDesktop VDI, par exemple.

Les licences de la solution Kaspersky Security for Virtualization sont proposées sous deux formes, afin de s'adapter aux besoins de votre entreprise et aux caractéristiques de votre infrastructure virtuelle : en fonction du nombre de machines virtuelles (bureaux et serveurs) ou en fonction du nombre de cœurs de processeurs physiques sur le serveur hôte.

Security for Mobile

Sécurité avancée, gestion et contrôle des smartphones et des tablettes

En 2016, sur une durée classique de trois mois, nous avons détecté plus de 3,5 millions de paquets d'installation malveillants, plus de 83 000 chevaux de Troie rançonneurs et plus de 27 000 chevaux de Troie bancaires, tous ciblant les appareils mobiles de nos clients.

Les logiciels et sites Web malveillants visant les appareils mobiles continuent à proliférer, de même que les attaques par hameçonnage, 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) a élargi la gamme d'appareils 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 EMPLOYÉS CONSTITUENT UN RISQUE POUR L'ENTREPRISE

Les employés utilisant leurs appareils mobiles dans un cadre professionnel, mais également personnel, augmentent les risques que la sécurité informatique d'une entreprise 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 PLATE-FORME N'EST À L'ABRI

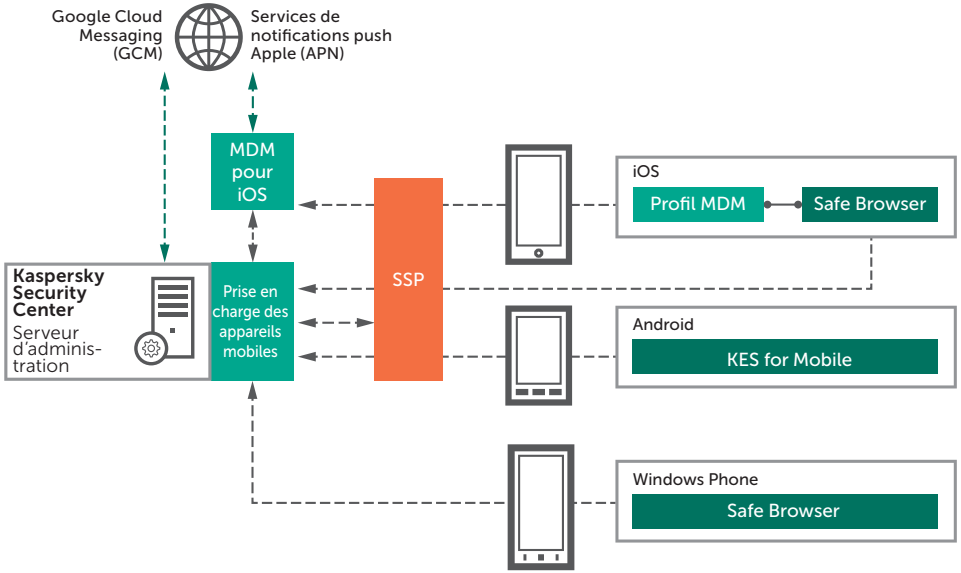
Les criminels ont toute une gamme de méthodes à leur disposition pour accéder sans autorisation aux appareils mobiles, et notamment les applications infectées, les réseaux wifi publics faiblement sécurisés, les attaques par phishing et les SMS infectés. Lorsqu'un utilisateur visite par inadvertance un 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 protection multi-niveaux et une large gamme de fonctionnalités de gestion des appareils mobiles (MDM) et de gestion des applications mobiles (MAM). Ces fonctions réduisent très nettement le temps nécessaire à la maintenance des appareils mobiles et proposent un accès mobile sécurisé aux systèmes de l'entreprise.

- **Sécurité mobile :** nos systèmes de sécurité pour appareils mobiles offrent une protection multi-niveaux contre les dernières menaces concernant les appareils mobiles, ainsi que des fonctionnalités antivol pouvant être commandées à distance.
- **Gestion des appareils mobiles :** l'intégration à toutes les plates-formes principales permet l'analyse et le contrôle à distance des appareils (OTA, « over-the-air »), ce qui permet d'améliorer considérablement la protection et la gestion des appareils basés sur les architectures Android, iOS et Windows Phone.
- **Gestion des applications mobiles :** les conteneurs isolés pour les applications et l'option d'effacement sélectif de la mémoire de l'appareil permettent d'empaqueter les informations professionnelles et personnelles stockées sur l'appareil de l'employé.

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



Architecture de la solution

DDoS Protection

Défense complète contre toutes les formes d'attaques DDoS

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

Kaspersky 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 :

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

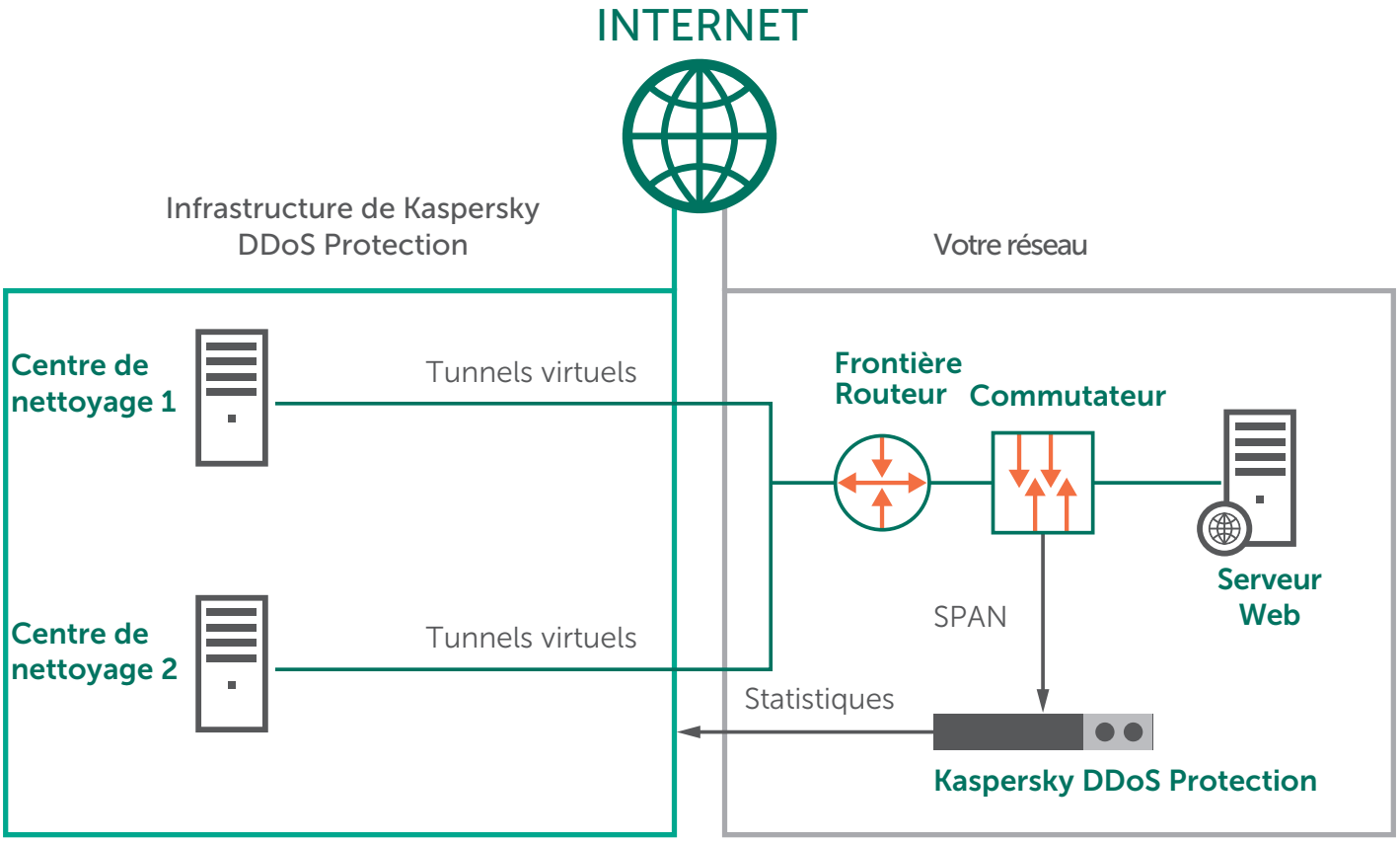


Schéma de Kaspersky DDos Protection Control

Industrial Cybersecurity

Protection spécialisée 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. Une récente étude a révélé que les cyberattaques étaient responsables de 35 % des dysfonctionnements des réseaux industriels.

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 technologiques 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

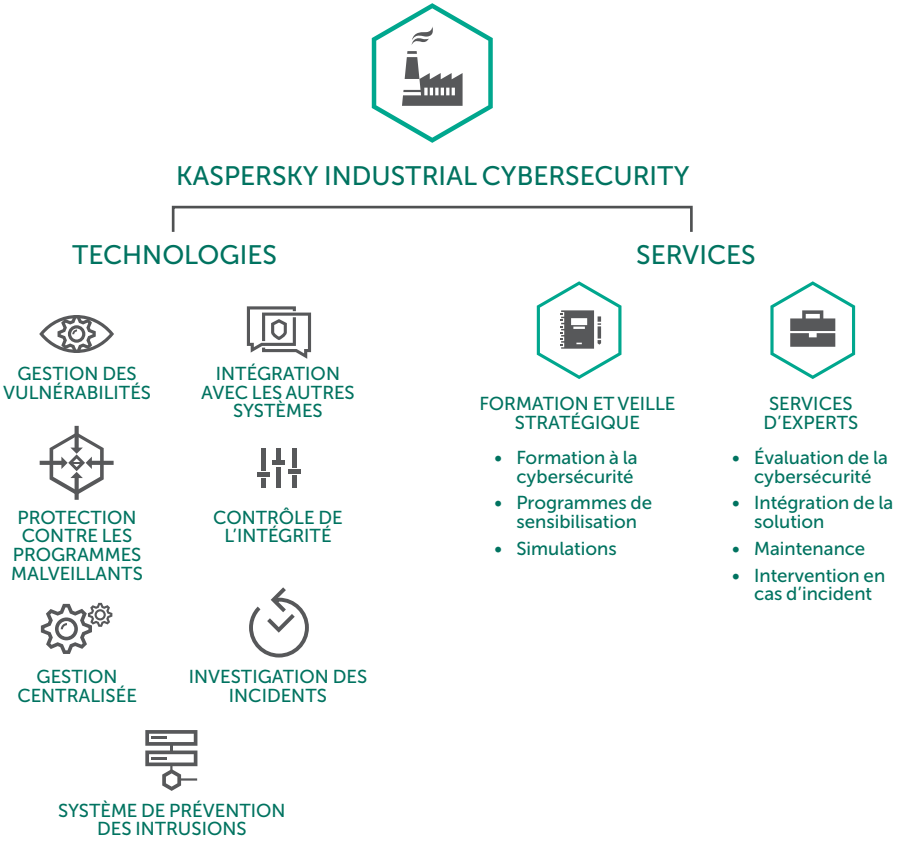
Kaspersky Industrial CyberSecurity est une gamme de technologies et de services conçus pour sécuriser tous les niveaux de l'industrie (serveurs SCADA, interfaces HMI, postes de travail des ingénieurs, API, connexions réseau et personnel) sans répercussions sur la continuité et la cohérence du processus technologique. 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 de sorte à 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 spécifique. 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 technologiques.



Fraud Prevention

Développement des services bancaires en ligne sans problèmes de sécurité ni de confort d'utilisation

À l'heure actuelle, les services bancaires en ligne constituent l'un des éléments essentiels nécessaires au développement des services financiers et à l'acquisition de clients. En revanche, ils ne sont pas uniquement devenus intéressants pour les clients, mais également pour les fraudeurs.

Les cybercriminels sont devenus progressivement adeptes du développement d'outils de plus en plus sophistiqués et capables de contourner les protections traditionnelles, de se frayer un chemin dans les systèmes bancaires, d'accéder aux comptes des clients, ainsi que d'effectuer et de falsifier des transactions.

Il était peut-être acceptable il y a quelques années de réagir à posteriori à une attaque de fraude, mais aujourd'hui ce mode de fonctionnement n'assure pas le degré de protection exigé par les banques et les clients.

Deloitte estime que le secteur des services financiers fait aujourd'hui face aux plus grands risques économiques liés à la cybersécurité et qu'il sera contraint de consacrer davantage de ressources à l'amélioration de son modèle de cybersécurité en matière de sécurité, de vigilance et de résistance.

LA SOLUTION : KASPERSKY FRAUD PREVENTION

Kaspersky Fraud Prevention renforce le système de sécurité existant d'une banque, ce qui permet d'offrir un nouveau niveau de protection contre la fraude. La solution protège les comptes numériques, les ordinateurs et les appareils mobiles des utilisateurs, ainsi que les systèmes de la banque. En protégeant les transactions et les comptes des clients, Kaspersky Fraud Prevention aide les banques à renforcer la fidélité de sa clientèle.

La solution Kaspersky Fraud Prevention appartient à une nouvelle génération de systèmes permettant d'analyser le comportement, les appareils et l'environnement des utilisateurs en temps réel. Grâce à l'apprentissage automatique, la solution détecte les scénarios de fraude avancés et les mécanismes de blanchiment d'argent. Elle permet également à l'équipe chargée de la lutte contre la fraude au sein de la banque de rassembler des informations précises sur chaque incident, notamment sur les identifiants utilisés pour accéder au compte.

Ces informations peuvent, par exemple, révéler qu'une banque n'est pas responsable d'un incident de fraude, ce qui réduirait considérablement les coûts propres aux dommages et à la compensation.

Kaspersky Fraud Prevention ajoute une couche défensive essentielle à la protection existante de la banque contre la fraude.

- **Kaspersky Fraud Prevention Clientless Malware Detection** propose des technologies côté serveur protégeant 100 % de vos clients, indépendamment de l'appareil ou de la plate-forme qu'ils utilisent. Le système permet à votre banque de détecter le plus tôt possible l'accès aux comptes par des clients infectés.
- **Kaspersky Fraud Prevention for Mobile** permet de protéger les utilisateurs accédant à leurs comptes bancaires depuis un appareil mobile (Android, iOS et Windows Phone).
- **Kaspersky Fraud Prevention for Endpoints** fonctionne sur les PC et Mac de vos clients et leur offre une protection efficace à la source contre les programmes malveillants et les attaques sur Internet.
- **Kaspersky Fraud Prevention Cloud** est un produit de détection des fraudes pour services bancaires mobiles et en ligne. Les principales fonctionnalités sont les suivantes : authentification selon le risque, analyse du comportement, détection continue des anomalies de session et biométrique passive basée sur l'apprentissage automatique et les modèles statistiques.

Cette solution complète de prévention de la fraude :

- ajoute une sécurité multicanal pour les opérations bancaires et les paiements numériques
- détecte de manière proactive et en temps réel les dispositifs de fraude avancés avant le traitement de la transaction
- protège tous les utilisateurs, indépendamment de l'appareil qu'ils utilisent
- assure une sécurité « fluide » pour une expérience utilisateur transparente
- aide les banques à renforcer la fidélisation de leurs clients, à en attirer de nouveaux et à encourager l'adoption et l'utilisation de services bancaires en ligne et mobiles à marge élevée.
- réduit les coûts grâce à l'automatisation et à l'apprentissage automatique.

Support et services professionnels

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

Lorsqu'un incident de sécurité entraîne l'interruption du système informatique, les conséquences peuvent affecter toutes les opérations d'une société. Pour éviter de telles éventualités, Kaspersky Lab propose une gamme de programmes d'assistance traitant à tout moment vos problèmes de sécurité informatique en tant que priorité absolue et assurant ainsi le bon fonctionnement de votre entreprise.

ASSISTANCE MSA ENTREPRISE

Les contrats de maintenance Kaspersky Lab MSA s'adressent aux entreprises qui dépendent de leur infrastructure informatique pour gérer la continuité de leur activité et l'exécution continue de leurs processus stratégiques. MSA Entreprise est spécifiquement conçu pour les grandes entreprises aux environnements complexes ayant besoin d'une assistance proactive, personnalisée et dédiée 24 h/24.

SERVICES PROFESSIONNELS

Conformément à notre méthodologie et à nos bonnes pratiques, nos experts en sécurité sont à votre disposition pour vous aider à déployer, configurer et mettre à niveau les solutions Kaspersky Lab dans l'ensemble de votre infrastructure informatique, ainsi qu'à appliquer votre politique de contrôle des changements.

- Service de mise en œuvre : propose une assistance et une prise en charge spécialisées pour assurer le déploiement transparent et sans faille des solutions Kaspersky Lab, vous garantir un fonctionnement conforme aux bonnes pratiques, mettre à votre disposition la meilleure configuration possible et vous permettre d'utiliser de façon optimale la console d'administration centralisée de Kaspersky Lab.
- Service de bilan technique : suite à un audit complet de votre environnement réseau et des paramètres de vos produits, nos experts élaborent un rapport exhaustif comprenant des recommandations sur la manière de renforcer la sécurité et/ou d'améliorer l'efficacité de la gestion de vos systèmes.

L'assistance et les services professionnels de Kaspersky Lab vous permettent de contacter des experts en sécurité qui savent comment résoudre vos problèmes rapidement, en toute sécurité et de manière efficace, ainsi que de bénéficier des éléments suivants :

- des accords de niveau de service pour les réponses aux incidents
- des correctifs personnalisés
- une réponse prioritaire aux incidents liés aux programmes malveillants
- des rapports de surveillance
- un interlocuteur unique

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 à 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. Notre entreprise est qualifiée de « leader » en matière de protection des postes de travail par les trois principaux analystes (Gartner, IDC et Forrester).

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

KASPERSKY lab