KASPERSKY lab

RECHERCHE MONDIALE SUR LA SÉCURITÉ INFORMATIQUE

VOS DONNÉES SONT MENACÉES : PROTÉGEZ-LES AVEC LE CHIFFREMENT

#EnterpriseSec
http://www.kaspersky.com/fr/entreprise-securite-it/

TABLE DES MATIÈRES

Vos données sont menacées : protégez-les avec le chiffrement 3

Procédure de limitation des risques 5

Chiffrement intégral de disques (FDE) 6

Chiffrement de fichiers (FLE) 8

À propos de Kaspersky Lab 11

VOS DONNÉES SONT MENACÉES : PROTÉGEZ-LES AVEC LE CHIFFREMENT

Pour les responsables informatiques, il peut s'avérer particulièrement difficile de rester en phase avec les exigences de l'entreprise. Parce que l'on vous demande de faire toujours plus avec moins de moyens, vous êtes soumis à une pression constante vous imposant de mettre en œuvre de nouvelles technologies afin d'améliorer la productivité et l'efficacité, tout en diminuant les coûts – tout cela en gérant également la menace grandissante de la cyber-criminalité. Et, comme si cela ne suffisait pas, vos collaborateurs sont devenus mobiles et doivent désormais quitter les murs protecteurs de l'entreprise. Confronté à la mobilité du personnel, un service informatique peut en arriver à se sentir particulièrement vulnérable.

Selon le Ponemon Institute, 62 % des collaborateurs d'une entreprise sont mobiles. Par ailleurs, dès 2015, ce chiffre devrait atteindre 85 %. Le personnel étant désormais mobile, les informations internes à l'entreprise le deviennent tout autant, générant un risque énorme de perte ou de vol de données. Le solide périmètre de sécurité que vous aviez mis en place pour protéger les systèmes et les réseaux de l'entreprise n'est désormais plus efficace ; les données ne sont plus à l'abri car elles se déplacent partout dans le monde. Il n'est guère étonnant que 80 % des professionnels de l'informatique d'entreprise considèrent les ordinateurs portables et autres appareils mobiles porteurs de données comme des menaces considérables pour les réseaux et les systèmes de l'entreprise.[1]

D'après une étude menée par Intel, 5 à 10 % de l'ensemble des ordinateurs portables seront perdus ou volés au cours de leur vie. **Faites le compte du nombre de vos collaborateurs déjà mobiles et voyez par vous-même : en moyenne, 63 % d'entre eux utilisent des appareils mobiles pour accéder aux données de l'entreprise**.

- 50 % d'entre eux, en moyenne, les utilisent pour accéder aux données sensibles.
- 63 % des appareils mobiles perdus ou volés contiennent des informations sensibles ou confidentielles.
- Un ordinateur portable est volé toutes les 53 secondes.
- 63 % des atteintes à la sécurité, vols et usages non autorisés sur le lieu de travail inclus, résultent de l'utilisation des appareils mobiles.[2]

L'explosion de la mobilité de l'entreprise signifie que vos données d'entreprise courent un risque conséquent.

En cas de perte ou de vol de votre appareil, si votre première réaction consiste à estimer le coût de remplacement du matériel, vous vous trompez de cible. Les recherches menées par le Ponemon Institute révèlent que le coût moyen d'un ordinateur portable perdu s'élève à 49 246 $, dont 2 % seulement sont imputables aux coûts de remplacement matériel. Quelle que soit la taille de l'entreprise, 80 % de ce coût sont consacrés à la résolution des problèmes générés par la fuite de données.

Les recherches de Kaspersky Lab révèlent que le coût moyen, pour l'entreprise, d'une seule atteinte à l'intégrité des données, s'élève à 649 000 $.[3]

1 & 2. Ponemon Institute, 2013 State of the Endpoint, décembre 2012
3. Enquête 2013 sur les risques liés à la sécurité informatique pour les entreprises mondiales, Kaspersky Lab, mai 2013

LE CHIFFREMENT FAIT PARTIE DES TECHNOLOGIES LES PLUS PROMETTEUSES EN MATIÈRE DE RÉDUCTION DU RISQUE DE FUITE DE DONNÉES CRITIQUES. ET SON EFFICACITÉ EST OPTIMALE LORSQU'IL EST INTÉGRÉ À UN SYSTÈME DE SÉCURITÉ COMPLET, ADAPTÉ À L'INFRASTRUCTURE INFORMATIQUE DE L'ENTREPRISE.

Si l'on tient compte du nombre croissant d'amendes infligées par les autorités pour violation des données, des préjudices causés à la réputation d'une société et de la désertion des clients, il n'est donc guère surprenant que les coûts liés à la perte d'un ordinateur portable aillent bien au-delà du simple remplacement d'équipements.

Dans un monde de plus en plus mobile, un simple périmètre de sécurité ne suffit plus à protéger la propriété intellectuelle de l'entreprise, les données sensibles, les réseaux et les systèmes. Si un appareil est perdu ou volé, les données qu'il contient peuvent elles aussi être volées : l'appareil est donc une cible de choix pour les criminels. Comment protégez-vous les données mobiles contre le vol, même si l'appareil est volé ?

LA RÉPONSE EST SIMPLE : LE CHIFFREMENT !

Le chiffrement est un processus qui code les informations de telle manière que seuls les utilisateurs autorisés peuvent les lire. Dans un schéma de chiffrement, les informations (en clair) sont codées à l'aide d'un algorithme de chiffrement qui les convertit en texte chiffré illisible. Ce processus s'effectue généralement à l'aide d'une clé de chiffrement, qui indique la façon dont les données doivent être encodées.

Les utilisateurs non autorisés peuvent être en mesure de voir le texte chiffré, sans pour autant découvrir les données d'origine. Les utilisateurs autorisés, en revanche, peuvent décoder le texte chiffré à l'aide d'un algorithme de déchiffrement qui nécessite généralement une clé secrète de déchiffrement, dont ils sont les seuls à détenir l'accès. Un schéma de chiffrement fait généralement appel à un algorithme de génération de clé afin de produire des clés de manière aléatoire.

Gartner estime que le coût d'une violation des données présentes sur un ordinateur portable perdu ou volé peut être 70 fois supérieur au coût du chiffrement appliqué à l'ensemble de l'entreprise.[4] Malgré tout, les recherches menées par Kaspersky Lab montrent que 35 % des entreprises exposent leurs données à des accès non autorisés car elles n'utilisent pas de technologies de chiffrement.[5]

Quel que soit le but recherché, les entreprises doivent protéger leurs données, leur propriété intellectuelle et leur réputation. Quels que soient leurs rôles et leurs secteurs d'activité, toutes les entreprises sont de plus en plus nombreuses à adopter le chiffrement comme mesure préventive de sécurisation des informations et stratégie de conformité réglementaire.

Deux types de chiffres peuvent être déployés, de façon indépendante ou conjointement : le chiffrement intégral de disques (FDE) et le chiffrement de fichiers (FLE). Les recherches de Kaspersky Lab ont montré que 40 % des entreprises mettent en place le FLE, alors que 39 % optent pour le FDE ; les 33 % restants ont adopté le chiffrement pour les supports amovibles.

4. John Girard, analyste chez Gartner, entretien avec Fierce Mobile IT, 25 octobre 2012.
5. Kaspersky Lab et B2B International, Rapport 2013 sur les risques informatiques mondiaux, mai 2013

PROCÉDURE DE LIMITATION DES RISQUES

Les recherches menées par Kaspersky Lab révèlent que les entreprises sont de plus en plus nombreuses à faire appel au chiffrement afin de mettre en place une stratégie efficace de prévention des pertes de données.

Protection contre les programmes malveillants (antivirus, Anti-spyware)	71 %	4 %
Gestion régulière des mises à jour de correctifs/logiciels	54 %	-9 %
Mise en œuvre de niveaux d'accès aux différents systèmes informatiques à l'aide de privilèges	52 %	4 %
Structures réseau (séparation des réseaux stratégiques des autres réseaux)	50 %	3 %
Contrôle des applications (seuls les programmes autorisés peuvent être exécutés sur les appareils)	45 %	N/A
Politique de gestion de la sécurité informatique dans des bureaux/succursales à distance	44 %	4 %
Contrôle des appareils (seuls les périphériques autorisés peuvent se connecter aux appareils)	41 %	N/A
Agent contre les programmes malveillants pour appareils mobiles	40 %	N/A
Chiffrement des fichiers et des dossiers	**40 %**	**N/A**
Chiffrement de toutes les données stockées (chiffrement intégral de disque dur)	**39 %**	**2 %**
Politique de sécurité distincte pour les ordinateurs portables	38 %	3 %
Politique de sécurité distincte pour les périphériques amovibles (USB, etc.)	37 %	0 %
Chiffrement des communications de l'entreprise	**37 %**	**-1 %**
Audit/vérification de la sécurité informatique de fournisseurs tiers	36 %	0 %
Gestion des clients (gestion du cycle de vie des ordinateurs)	34 %	-1 %
Chiffrement des données sur les périphériques amovibles	**33 %**	**2 %**
Politique de sécurité distincte pour les smartphones/ tablettes	32 %	0 %
Gestion des appareils mobiles (MDM)	31 %	-2 %

N/A nouvelles questions soulevées **en 2013**

Ce diagramme montre le pourcentage d'organisations ayant entièrement déployé différentes mesures de sécurité

Baisse significative d'une année sur l'autre

Hausse significative d'une année sur l'autre

CHIFFREMENT INTÉGRAL DE DISQUES (FDE)

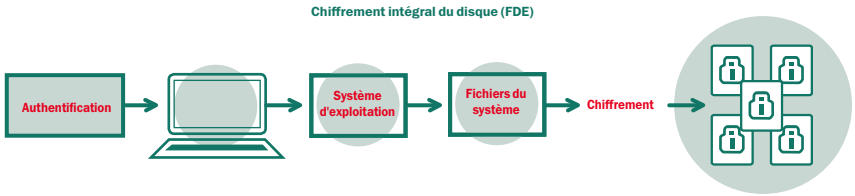
La technologie de chiffrement intégral du disque (FDE) représente l'une des méthodes les plus efficaces adoptées par les entreprises pour les protéger du vol ou de la perte de données. Quoi qu'il arrive à un appareil, le FDE permet aux entreprises de s'assurer que toutes les données sensibles sont totalement illisibles et inutiles pour les criminels ou les indiscrets.

Le FDE chiffre les données en circulation (autrement dit, toutes les données présentes sur le disque dur), du démarrage au chargement du système d'exploitation et sur les autres disques durs installés. En fait, chaque fichier (fichiers temporaires inclus) présent sur chaque secteur du disque est chiffré. Seuls les utilisateurs authentifiés peuvent accéder au système, à l'aide d'un mot de passe et/ou d'un jeton. Cette technologie peut également être appliquée aux supports amovibles comme les clés USB. Le FDE prend en charge tout un éventail de configurations et peut être géré et contrôlé par les administrateurs système.

Le fonctionnement du FDE s'appuie sur un schéma de pré-démarrage. Ainsi, il peut protéger les données dans les secondes qui suivent l'activation du bouton d'alimentation de l'appareil. Le logiciel chiffre tous les disques sélectionnés et installe un module d'authentification dans l'environnement de démarrage. Lorsqu'un ordinateur est démarré, le système d'exploitation se charge automatiquement dans un environnement chiffré, afin que le chiffrement n'affecte quasiment pas les performances de l'ordinateur.

Toutes les activités de chiffrement et de déchiffrement s'exécutent de façon routinière, sans que l'utilisateur en ait conscience, et quel que soit le logiciel utilisé. Les opérations de lecture/écriture s'effectuent dans un environnement totalement protégé. Tout ce qui est présent sur le disque dur est sécurisé, de l'espace de pagination au système, à la page, en passant par les fichiers d'hibernation et temporaires, qui peuvent souvent contenir des données confidentielles importantes. En cas de perte du mot de passe, les informations peuvent toujours être déchiffrées à l'aide de clés privées connues uniquement par l'administrateur système. Les appareils mobiles équipés du FDE peuvent grandement limiter le risque de violation des données en cas de vol ou de perte.

La fonctionnalité FDE fait partie de la solution Kaspersky Endpoint Security for Business. Les administrateurs système peuvent la gérer du démarrage au de façon centralisée, depuis la console de gestion du démarrage au chargement du système d'exploitation et sur ... Kaspersky Security Center.



LE CHIFFREMENT INTÉGRAL DU DISQUE OFFRE DE NOMBREUX AVANTAGES EN MATIÈRE DE SÉCURITÉ INFORMATIQUE :

- **Chiffrement appliqué aux données sensibles** : le FDE évite à l'utilisateur final de décider de chiffrer ou non ses données. Tous les fichiers présents sur le disque dur sont automatiquement chiffrés et protégés par un mot de passe, y compris les fichiers temporaires, qui contiennent souvent des données sensibles. L'utilisateur final n'a pas la possibilité de contourner ce processus.

- **Sécurité** : le FDE empêche tout accès non autorisé aux données grâce à un mécanisme d'authentification/mot de passe. Lorsque l'authentification/le mot de passe correct(e) est présenté(e), le système récupère la clé nécessaire au déchiffrement des fichiers sur le disque dur. Vous bénéficiez ainsi d'une strate de sécurité supplémentaire car les données peuvent être rendues inutilisables immédiatement après la destruction de la clé de cryptographie.

- **Gestion centralisée des clés** : les clés de chiffrement peuvent être conservées en un point central accessible uniquement à l'administrateur système.

- **Gestion centralisée du chiffrement** : les systèmes de FDE permettent de gérer toutes les fonctions depuis un emplacement central au sein de l'entreprise. Ceci inclut les fonctions telles que la gestion des clés de chiffrement, le contrôle d'accès aux appareils mobiles, les verrouillages, si nécessaire, les rapports et la récupération des mots de passe oubliés.

- **Simplicité et flexibilité** : les systèmes de FDE sont totalement transparents pour l'utilisateur final et intégralement automatiques. Une fois l'autorisation accordée, le processus de chiffrement/déchiffrement se déroule simplement, sans affecter les opérations de l'utilisateur.

- **Récupération centralisée des données** : en cas d'oubli du mot de passe ou de détérioration du support des données, celles-ci peuvent quand même être récupérées et déchiffrées grâce à la procédure spéciale de récupération d'urgence gérée au niveau central.

Même si le FDE assure une protection étendue des données présentes sur les appareils perdus ou volés, il ne protège pas les données en circulation – les données partagées électroniquement entre les appareils, par e-mail par exemple. C'est pourquoi de nombreuses entreprises mettent souvent en place un chiffrement au niveau des fichiers.

CHIFFREMENT DES FICHIERS (FLE)

GRÂCE AU FLE, DES FICHIERS OU DES RÉPERTOIRES INDIVIDUELS SONT CHIFFRÉS PAR LE SYSTÈME DE FICHIERS LUI-MÊME, CONTRAIREMENT AU CHIFFREMENT INTÉGRAL DU DISQUE, QUI CHIFFRE LA TOTALITÉ DE LA PARTITION OU DU DISQUE SUR LEQUEL RÉSIDE LE SYSTÈME DE FICHIERS. LE FLE NE CHIFFRE PAS TOUTES LES INFORMATIONS PRÉSENTES SUR LE DISQUE OU L'APPAREIL PORTABLE COMME LE FDE.

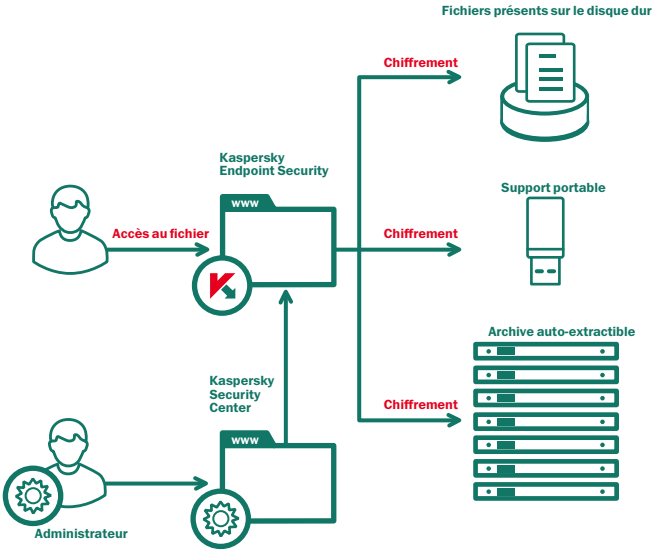
Le chiffrement des fichiers (FLE) permet de chiffrer les données présentes dans des fichiers et des dossiers spécifiques d'appareils désignés. Ainsi, les informations sélectionnées sont illisibles pour les individus non autorisés, quel que soit l'emplacement où ces fichiers sont stockés. Le FLE permet aux administrateurs système de chiffrer automatiquement les fichiers en fonction d'attributs tels que l'emplacement ou le type de fichier.

Grâce au FLE, des fichiers ou des répertoires individuels sont chiffrés par le système de fichiers lui-même, contrairement au chiffrement intégral du disque, qui chiffre la totalité de la partition ou du disque sur lequel réside le système de fichiers. Le FLE ne chiffre pas toutes les informations présentes sur le disque ou l'appareil portable comme le FDE. En revanche, il permet aux administrateurs de choisir les données à chiffrer (ou non), en s'appuyant sur des règles faciles à mettre en place grâce à une interface logicielle conviviale.

La technologie du FLE permet aux administrateurs du système de personnaliser totalement les fichiers à chiffrer. Cette personnalisation peut se faire manuellement ou automatiquement ; certaines solutions proposent des outils spécialement pré-configurés permettant de chiffrer facilement et rapidement les fichiers, de façon fiable. Les politiques d'accès aux informations granulaires sont facilement appliquées. Par exemple, les administrateurs peuvent désirer appliquer automatiquement le chiffrement aux feuilles de calculs financières, mais pas aux feuilles de calculs plus générales. Les règles de chiffrement peuvent être personnalisées de façon à décider de ce qui doit être chiffré ou pas, comme dans les exemples ci-dessous :

- **Fichiers présents sur des disques durs locaux** : les administrateurs peuvent créer des listes de fichiers à chiffrer par nom, extension ou répertoire.
- **Fichiers présents sur un support portable** : créez une politique de chiffrement par défaut pour appliquer le chiffrement à tous les appareils portables. Appliquez ces mêmes règles à chaque appareil ou précisez votre action en créant différentes règles applicables aux différents appareils.
- **Choix des contenus à chiffrer** : le FLE permet d'appliquer différentes règles de chiffrement aux différentes situations rencontrées. Par exemple, vous pouvez choisir de chiffrer tous les fichiers présents sur des appareils portables ou uniquement les nouveaux fichiers. Vous pouvez également activer le mode de chiffrement portable pour les fichiers chiffrés utilisés sur les PC qui ne sont pas équipés de la solution Kaspersky Endpoint Security for Business.
- **Fichiers d'application** : chiffrez automatiquement tout fichier créé ou modifié par une application.
- **Archives chiffrées auto-extractibles** : les fichiers ajoutés aux archives chiffrées auto-extractibles peuvent être déchiffrés à l'aide d'un mot de passe sur les PC non équipés de la solution Kaspersky Endpoint Security.

LE CHIFFREMENT DE FICHIERS EST TOTALEMENT TRANSPARENT : AINSI, TOUTE PERSONNE AYANT ACCÈS AU SYSTÈME DE FICHIERS PEUT VISUALISER LES NOMS (ET ÉVENTUELLEMENT LES AUTRES MÉTADONNÉES) DES FICHIERS ET DES DOSSIERS CHIFFRÉS, Y COMPRIS CEUX DES FICHIERS ET DES DOSSIERS CONTENUS DANS LES DOSSIERS CHIFFRÉS, S'ILS NE SONT PAS PROTÉGÉS À L'AIDE DE FONCTIONS DE CONTRÔLE D'ACCÈS AU SYSTÈME D'EXPLOITATION. LE CHIFFREMENT DE FICHIERS/DOSSIERS EST UTILISÉ SUR TOUS LES TYPES DE STOCKAGE DES APPAREILS DE L'UTILISATEUR FINAL.



Le chiffrement de fichiers implique de chiffrer les fichiers individuels présents sur un support de stockage, en ne donnant accès aux données chiffrées qu'une fois l'authentification réussie. Le chiffrement de dossiers applique les mêmes principes aux dossiers individuels plutôt qu'à des fichiers spécifiques.

Le chiffrement de fichiers est totalement transparent : ainsi, toute personne ayant accès au système de fichiers peut visualiser les noms (et éventuellement les autres métadonnées) des fichiers et des dossiers chiffrés, y compris ceux des fichiers et des dossiers contenus dans les dossiers chiffrés, s'ils ne sont pas protégés à l'aide de fonctions de contrôle d'accès au système d'exploitation. Le chiffrement de fichiers/dossiers est utilisé sur tous les types de stockage des appareils de l'utilisateur final.

Le chiffrement de fichiers s'applique via une solution qui repose sur un pilote, dotée d'un module de cryptographie spécial qui intercepte toutes les opérations d'accès aux fichiers. Lorsqu'un utilisateur tente d'accéder à un fichier chiffré (ou à un fichier contenu dans un dossier chiffré), le logiciel de FLE s'assure que cet utilisateur a été authentifié ou ouvre une boîte de dialogue de saisie du mot de passe en cas d'accès à une archive chiffrée auto-extractible. Une fois l'authentification effectuée, le logiciel déchiffre le fichier choisi.

Étant donné que le FLE déchiffre un fichier à la fois, l'impact de cette opération sur les performances de l'appareil est minime. Le chiffrement de fichiers/dossiers est surtout utilisé sur les fichiers de données utilisateur, comme les documents de traitement de texte et les feuilles de calculs. Les solutions de FLE ne peuvent pas chiffrer l'exécution du système d'exploitation ou les fichiers d'hibernation.

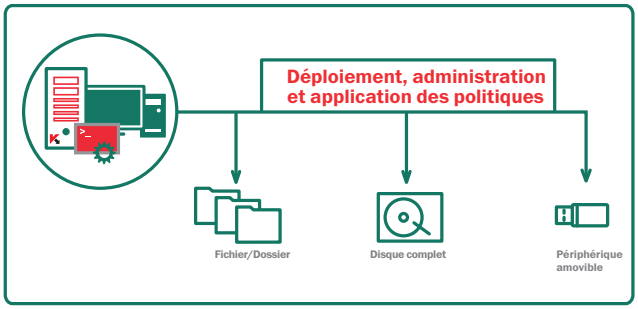
Le FLE offre de nombreux avantages en matière de sécurité informatique :

- **Flexibilité** : des règles personnalisées de choix et d'emplacement du chiffrement (fichiers, extensions et répertoires) peuvent être créées et appliquées à différents cas et exigences d'utilisation.
- **Support portable** : créez des règles de chiffrement spéciales applicables à tous les appareils portables connectés à un PC/ordinateur portable. Appliquez ces mêmes règles à toute l'entreprise ou choisissez des options adaptées à chaque appareil.
- **Chiffrement logiciel transparent** : chiffrez les données créées ou modifiées par n'importe quel logiciel s'exécutant sur le disque dur. Définissez les droits d'accès aux fichiers chiffrés en fonction des applications ou exigez l'enregistrement des fichiers au format chiffré.
- **Gestion centrale** : toutes les fonctions du FLE peuvent être gérées de façon centrale, y compris les fonctions de gestion des règles, de gestion des droits et de gestion des clés.

Protégez vos données en toute simplicité et de manière sécurisée grâce à la technologie de chiffrement de Kaspersky

- DISQUE DUR INTÉGRAL
- FICHIERS/DOSSIERS
- APPAREILS AMOVIBLES/INTERNES

ADMINISTRATION VIA UNE CONSOLE DE GESTION SIMPLE ET UNIQUE.



RÉSUMÉ

Actuellement, le personnel mobile de votre entreprise ne doit pas représenter une menace supplémentaire pour la sécurité de vos données. Le chiffrement constitue un moyen logique de sécuriser les données présentes sur des appareils mobiles vulnérables. Il peut cependant présenter des défis supplémentaires en termes de gestion et de ressources. La manière la plus simple d'éviter cela consiste à mettre en place le chiffrement dans le cadre d'une plate-forme unique de sécurité, associant des technologies et des outils totalement intégrés, comme des outils fiables de gestion des programmes malveillants, une gestion efficace des systèmes, une gestion et un chiffrement des appareils mobiles, dans une solution facile à exploiter. Vous bénéficiez alors d'une visibilité parfaite sur les risques courus par tous les appareils de l'entreprise, à partir d'une console unique, à un coût unique.

Kaspersky Endpoint Security for Business (KESB) assure une protection fiable des données présentes sur tous les appareils depuis une console unique, ce qui facilite grandement les opérations et limite les risques pour votre entreprise. Par ailleurs, l'exploitation du réseau Kaspersky Security Network et l'implication de nos équipes Global Research and Analysis Teams (GReAT) connues dans le monde entier nous offrent une vue étendue des millions de menaces présentes aux quatre coins du monde. Grâce à cette veille stratégique, nous sommes en mesure d'identifier et, la plupart du temps, de prévoir les incidents de sécurité de façon à aider les entreprises à se protéger plus efficacement et à réagir plus rapidement si leurs systèmes informatiques sont compromis. Nous concentrons nos efforts sur la résolution des problèmes de sécurité informatique à l'échelle internationale, de la protection des infrastructures critiques à la prévention des fraudes et aux services de veille en passant par la mobilité des entreprises et la sécurisation des environnements virtuels.

Kaspersky Lab ne cesse d'anticiper et de prévenir les incidents menaçant la sécurité informatique des entreprises en réduisant les risques auxquels elles sont confrontées aujourd'hui et auxquels elles devront faire face à l'avenir.

À propos de Kaspersky Lab

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 16 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab, dont la société de gestion est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et apporte une protection à plus de 300 millions d'utilisateurs.

Plus d'informations sur www.kaspersky.fr

* Selon une enquête menée par IDC en 2012, l'entreprise occupe la quatrième place du classement par chiffre d'affaires des fournisseurs de solutions de sécurité des terminaux à l'échelle mondiale. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les fournisseurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.