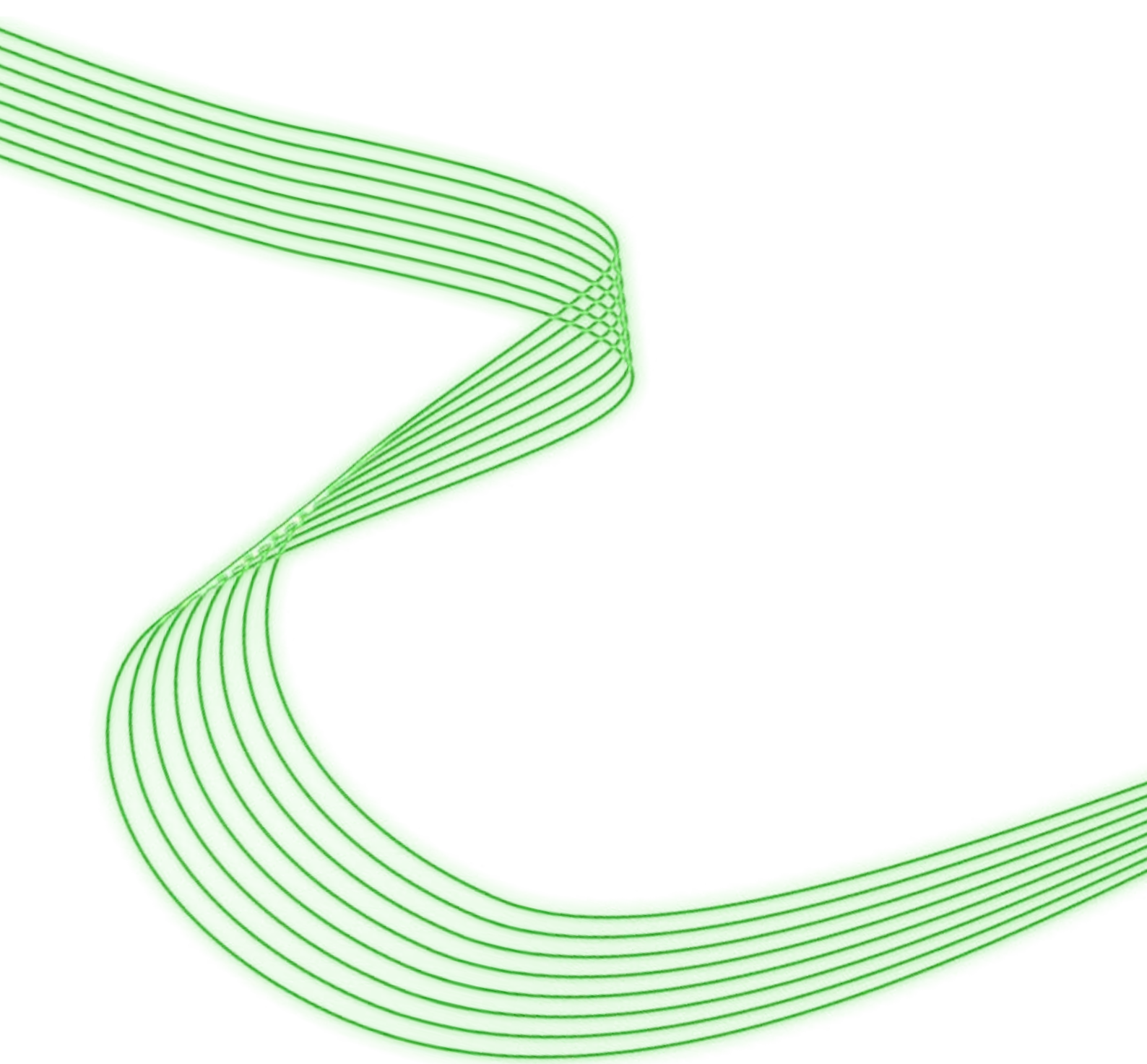


POURQUOI LA COMPLEXITÉ EST LE PIRE ENNEMI DE LA SÉCURITÉ INFORMATIQUE.

La complexité crée de nouveaux défis en termes de sécurité.
Comment y faire face?

Avec Kaspersky, maintenant c'est possible !
kaspersky.fr/business

KASPERSKY lab

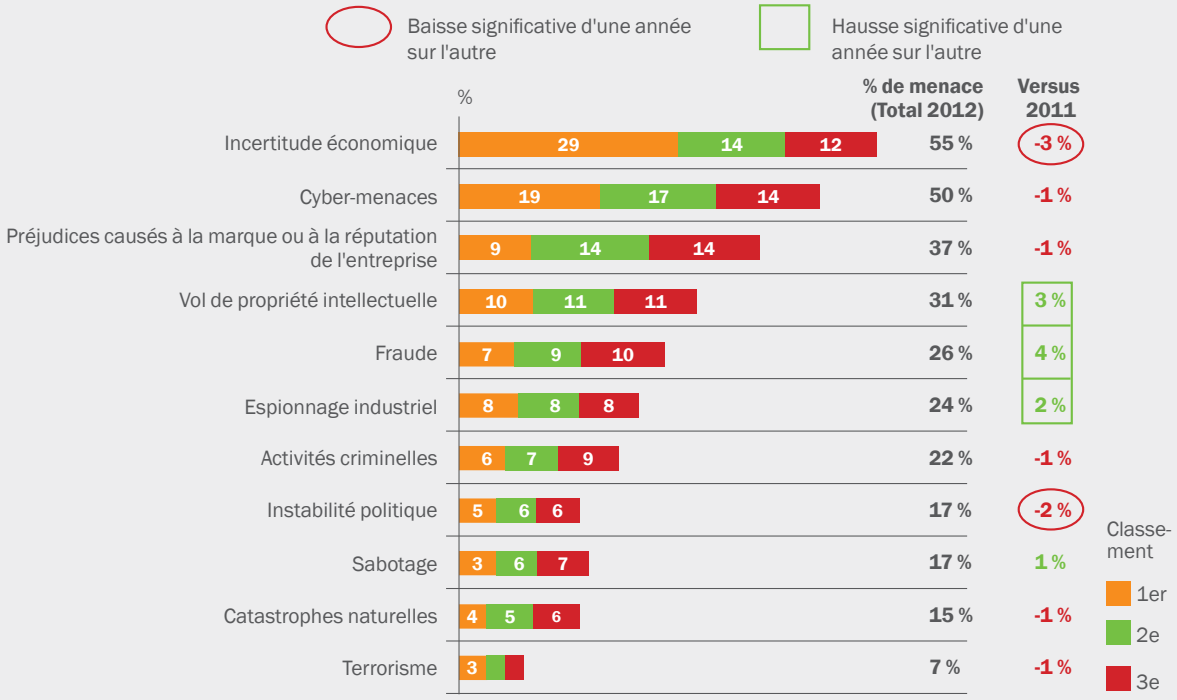
Synthèse

1.0

Alors que les entreprises du monde entier poursuivent leur quête d'agilité, d'efficacité et d'innovation, il leur faut dans le même temps réduire les coûts, améliorer la productivité et être toujours plus compétitives. Rien de bien nouveau si ce n'est que les services informatiques sont finalement les premiers concernés par ces différentes missions.

Ces nouvelles exigences ajoutent un niveau de complexité et viennent allonger la liste des tâches déjà gérées par les responsables informatiques. Or, avec cet accroissement de la complexité, le risque de laisser passer une vulnérabilité système telle qu'une application dépourvue de correctifs ou l'ajout d'un périphérique sur le réseau augmente plus que jamais. Autant de négligences qui peuvent à leur tour entraîner des problèmes de sécurité majeurs. Les entreprises ont conscience de ces difficultés. De ce fait, lorsque Kaspersky Lab a recueilli les opinions et expériences de plus de 3 300 professionnels informatiques expérimentés dans 22 pays à l'occasion de l'**enquête 2012 sur les risques informatiques au niveau mondial**, il en est ressorti sans surprise que les entreprises considèrent les cyber-menaces comme le deuxième plus grand risque après l'incertitude économique (voir l'illustration 1).

Illustration 1 : Principaux risques actuels pour les entreprises[1]



Les principaux domaines technologiques qui nécessitent des ressources et des outils de gestion supplémentaires sont les fonctionnalités de sécurité des appareils mobiles, de chiffrement des données et de contrôle (des applications, du Web et des périphériques) ainsi que la gestion des systèmes ; la tâche souvent manuelle de mise à jour des correctifs arrive en tête des préoccupations dans l'enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial (voir l'illustration 2).

1 Source : enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial

« Une sécurité informatique efficace correspond toujours à un juste équilibre entre risques, coûts et commodité, sachant que seule une compréhension profonde du premier de ces facteurs permet une évaluation précise des deux autres aspects. Mon inquiétude, confirmée par les conclusions de l'enquête, concerne l'augmentation actuelle des risques à un rythme plus rapide que ne l'imaginent les entreprises. »
Chris Christiansen, VP Security Products & Services chez IDC[3]

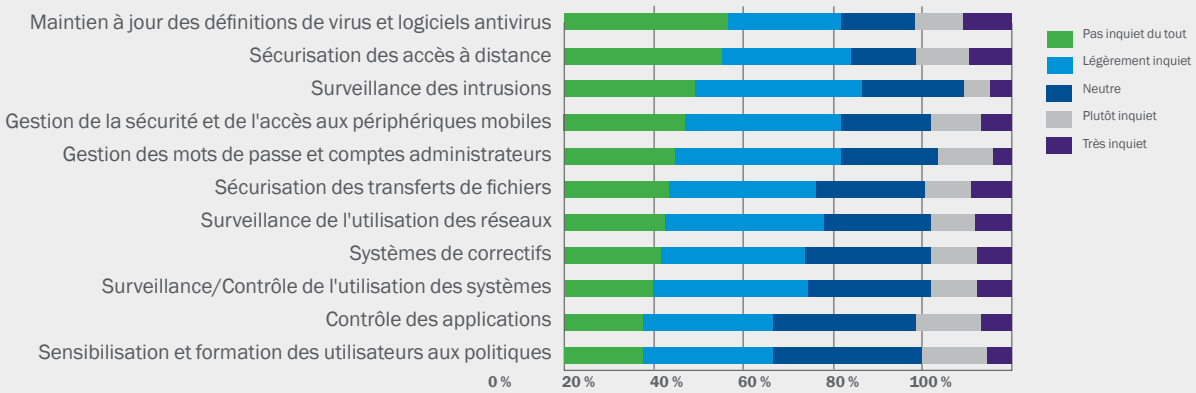
Les solutions de sécurité informatique actuelles peuvent exacerber les problèmes associés à la complexité dans la mesure où il s'agit généralement de solutions ponctuelles destinées à résoudre des problèmes spécifiques tels que la gestion des périphériques mobiles ou le chiffrement. Au mieux, elles sont « connectées » ; au pire, elles ne communiquent tout simplement pas entre elles. Dans ce cas, les administrateurs informatiques sont amenés à jongler entre les tableaux de bord pour mettre en œuvre des politiques, vérifier le statut des terminaux et appliquer des correctifs aux applications. Conséquence : l'apparition facilitée de failles de sécurité.

Une grande entreprise internationale peut investir dans des technologies à grande échelle, avec des ressources dédiées et spécialisées garantissant une sécurité informatique parfaitement étanche. Mais cette option n'est tout simplement pas accessible à la plupart des PME qui doivent résoudre ces mêmes problèmes avec une équipe informatique beaucoup plus réduite.

Les entreprises sont prises au piège entre des problématiques concurrentes : l'accroissement des données stratégiques, la gestion d'un environnement plus complexe et des facteurs de risque externes qui ne cessent de prendre de l'ampleur.

Cette situation est mise en évidence dans les résultats de l'enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial[2], commentés en ces termes par Chris Christiansen, VP Security Products & Services chez IDC : *« Une sécurité informatique efficace correspond toujours à un juste équilibre entre risques, coûts et commodité, sachant que seule une compréhension profonde du premier de ces facteurs permet une évaluation précise des deux autres aspects. Mon inquiétude, confirmée par les conclusions de l'enquête, concerne l'augmentation actuelle des risques à un rythme plus rapide que ne l'imaginent les entreprises. »*

Illustration 2 : Dans quelle mesure les problèmes de sécurité informatique suivants au sein de votre entreprise vous inquiètent-ils ?[2]



Pour les entreprises, bien conscientes des éléments qu'il leur faut sécuriser (et même de la manière d'y parvenir), une nouvelle approche est nécessaire. Une approche qui rompe avec les normes et contraintes existantes et qui permette aux équipes informatiques à court de ressources de construire et de gérer un dispositif de sécurité informatique d'une portée élargie.

Le présent livre blanc s'intéresse aux véritables défis auxquels les entreprises sont confrontées, ainsi qu'aux nouvelles menaces et aux nouveaux problèmes de sécurité informatique en résultant. Il apparaît de plus en plus que la seule protection contre les programmes malveillants ne suffit plus. C'est pourquoi ce livre blanc explore la nouvelle approche de sécurité informatique à adopter pour réagir efficacement à l'évolution des menaces et aux nouvelles méthodes de travail.

2 Source : enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial
3 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux

Objectifs des entreprises et origines de la problématique actuelle

2.0

La nécessité d'une nouvelle approche de la sécurité informatique est issue des changements imposés aux équipes informatiques par leurs entreprises. Certains d'entre eux sont liés à des impératifs technologiques, mais tous découlent en fin de compte d'une volonté fondamentale de réduire les coûts, de faire preuve d'une plus grande agilité et d'accroître la productivité.

2.1 Technologie
La technologie est plus que jamais le moteur de l'économie et cette situation a conduit à la création d'un nombre sans précédent de systèmes et plates-formes dont nous sommes tous dépendants pour travailler efficacement. Les entreprises de toutes tailles adoptent les technologies rapidement et cela dans de nombreux domaines de spécialisation. Les outils de collaboration sont utilisés massivement pour accélérer la prise de décision et réduire les temps et frais de déplacement, tandis que les entreprises fournissent à leurs employés tout un éventail d'appareils mobiles.

Tout cela génère encore plus de données et crée une nouvelle génération de « terminaux » et de points d'entrée potentiels pour les cybercriminels.

2.2 Manque de préparation et de ressources ?
La gestion de tous ces éléments est un fardeau qui incombe aux équipes informatiques. Celles-ci doivent ainsi réaliser un travail accru et largement plus complexe avec bien souvent des ressources identiques voire inférieures.

Les responsables et administrateurs informatiques multiplient les casquettes. Multitâches, ils doivent être en mesure de maîtriser rapidement toutes sortes de nouvelles technologies. Le matin, ils reconfigurent des serveurs, le midi ils ajustent les règles des pare-feu et les listes de contrôle d'accès. L'après-midi, ils passent en revue les paramètres de configuration des périphériques mobiles pour que le nouveau smartphone ou la nouvelle tablette du PDG puisse recevoir les e-mails et accéder au réseau. Et avant de quitter le bureau, ils s'emploient à résoudre les conflits de conversion d'adresses réseau sur les routeurs de bordure. La routine, me direz-vous ? En réalité, toute la difficulté de ces activités naît de la multitude des nouvelles technologies et exigences qui n'existaient tout simplement pas il y a encore quelques années.

2.3 Évolution des habitudes de travail
Les employés sont désormais habitués à avoir à portée de main des technologies fonctionnelles hautement conviviales. Cette nouvelle génération trouve rapidement des outils de collaboration, des applications et des périphériques à utiliser dans un environnement professionnel.

Elle a l'habitude d'accéder à des services Web où qu'elle soit et d'avoir au bout des doigts les applications, informations et ressources dont elle a besoin, sans assistance ou, plus important encore, sans qu'un service informatique ne lui impose une manière de travailler ou des outils de travail. Effet secondaire de la « consumérisation » des technologies, cette situation a généré une demande implacable d'agilité côté entreprises. Une attente à laquelle le mode de livraison de services informatiques traditionnel des entreprises répond difficilement.

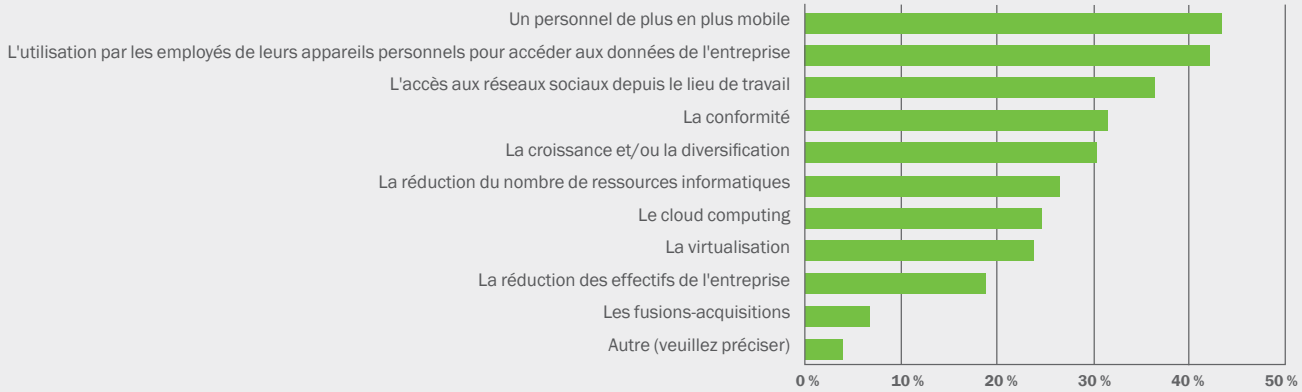
Plutôt que de combattre cette tendance, il s'agit plus aujourd'hui de trouver un moyen de la contrôler.

2.4 Mobilité

Au troisième trimestre 2012, IDC annonçait la livraison de 444,5 millions de smartphones à des utilisateurs du monde entier, un chiffre en hausse de 2,4 % par rapport à l'année précédente.[4] Un grand nombre de ces périphériques mobiles pénètrent la sphère professionnelle et les utilisateurs finaux voient la mobilité comme un moyen de fusionner leurs vies numériques professionnelle et personnelle.

En mars 2012, Kaspersky a mené, en collaboration avec les analystes de Bathwick Group, une étude mondiale intitulée **Préparation à la sécurité dans un contexte technologique en mutation (voir l'illustration 3)**, dont les résultats ont révélé que la mobilité est actuellement la principale source de préoccupation des professionnels de l'informatique à travers le monde. L'augmentation du nombre d'employés (souvent des employés expérimentés) apportant leur propre appareil au travail, accédant au réseau de l'entreprise et utilisant les informations de celle-ci signe l'échec de l'informatique dans la lutte pour le contrôle.

Illustration 3 : Quels défis constituent le principal casse-tête de sécurité pour votre entreprise ?[5]



Plutôt que de combattre cette tendance, il s'agit plus aujourd'hui de trouver un moyen de la contrôler. Cela n'est pas une mince affaire, compte tenu du nombre considérable de types de périphériques, de systèmes d'exploitation et d'applications mobiles ainsi que de l'« invisibilité » procurée par le fait que les employés puissent accéder à tout ce dont ils ont besoin par une simple connexion, sans fil ou câblée. L'augmentation de la complexité signifie un plus grand nombre d'éléments à gérer.

La combinaison des changements informatiques et de l'évolution des habitudes de travail et des besoins commerciaux crée une véritable tension dans la recherche d'un équilibre entre ressources, coûts et sécurité.

4 Le marché mondial des smartphones devrait croître de 55 % en 2011 et s'approcher du chiffre d'un milliard d'appareils déployés en 2015, selon IDC, le 9 juin 2011, http://www.idc.com/getdoc.jsp?containerId=prUS22871611
5 Source : Bathwick Group, « Préparation à la sécurité dans un contexte technologique en mutation », mars 2012

Menaces :
une nouvelle ère de sophistication

3.0

- Plus de 67 millions de menaces uniques dans la base de données Kaspersky[6]
- Le nombre de menaces augmente de 125 000 par jour[6]
- 140 nouvelles attaques contre les appareils mobiles chaque jour[6]
- 91 % des entreprises ont subi au moins une menace au cours des 12 derniers mois[7]

Deux mots résument bien l'évolution des risques en matière de cyber-sécurité au cours des dernières années : volume et sophistication. En témoigne l'enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial dans laquelle 91 % des entreprises indiquent avoir été confrontées à au moins une attaque au cours des 12 derniers mois.

Le niveau de sophistication observé dans les programmes malveillants a progressé, à tel point que nombreux sont ceux qui pensent qu'une solution anti-malware « traditionnelle » ne suffit plus. Cas extrêmes, Stuxnet et Flame ont fait la une de l'actualité, non seulement pour les dégâts causés mais aussi pour leur capacité à passer inaperçus sur une durée aussi prolongée. Flame, par exemple, existe depuis des années mais n'a été formellement identifié qu'en mai 2012.

3.1 Des menaces toujours plus sophistiquées

Ces exemples soulignent bien une hausse du « niveau d'entrée » pour les cybercriminels : les virus sont plus sophistiqués et exploitent les vulnérabilités dans l'intention explicite de voler des données sensibles.

Les comptes bancaires des entreprises sont une cible de choix du fait de leurs soldes élevés et du manque fréquent de mesures de sécurité prises par leur titulaire. Ceci explique certainement le volume croissant de chevaux de Troie et de programmes malveillants comme Zeus, qui volent des informations et permettent aux pirates de compromettre les finances d'une société.

Cette tendance est corroborée par l'explosion des menaces persistantes avancées. Les gouvernements et les entreprises internationales ne sont pas les seules cibles des attaques de programmes malveillants hautement sophistiqués, les petites entreprises sont exposées à un risque tout aussi important. Par ailleurs, à mesure que les cybercriminels recourent davantage à ce type de menaces, le risque de dommages collatéraux augmente, si bien que même des entreprises non spécifiquement visées peuvent subir les conséquences de ces attaques.

3.2 Plus haut dans la pile d'infrastructure

Ce degré de sophistication et de détermination change entièrement la donne concernant les besoins de sécurité informatique moyens des entreprises. Le point de départ d'une grande partie des attaques actuelles est l'exploitation des vulnérabilités des applications couramment utilisées. Autrefois, Windows lui-même était le principal centre d'attention des individus à la recherche de vulnérabilités susceptibles d'être utilisées pour installer du code malicieux sur un ordinateur. Mais la diffusion régulière de mises à jour de sécurité par Microsoft au cours des dernières années a conduit les cybercriminels à s'intéresser à d'autres applications. Tant et si bien que Windows ne figure même plus parmi les 10 packages logiciels les plus vulnérables (voir les illustrations 4 et 5). Malheureusement, de nombreuses applications demeurent dépourvues de correctifs pendant des périodes prolongées.

6 Source : Kaspersky Lab
7 Source : enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial

Selon securelist.com, plus de 80 % de l'ensemble des vulnérabilités ciblent Java et Adobe Acrobat Reader[8]. Non seulement Java est installé sur un grand nombre d'ordinateurs (1,1 milliard selon Oracle), mais les mises à jour sont installées à la demande et non de manière automatique. Dans le cas d'Adobe Acrobat Reader, seules les versions récentes incluent des mises à jour automatiques. Les utilisateurs ont pris l'habitude de télécharger des applications sur leurs PC et smartphones, créant ainsi des dizaines d'applications gérées et non gérées, chacune d'elles comportant un certain nombre de vulnérabilités potentielles.

La diversité croissante des appareils et plates-formes d'exploitation sur lesquels les entreprises effectuent des transactions de données ne fait qu'amplifier le défi de la sécurité. Pour résumer, plus d'éléments à gérer signifie plus de failles à combler.

Le volume de failles de sécurité s'est déplacé vers ces plates-formes, mais le nombre croissant de systèmes d'exploitation et les dizaines de milliers d'applications créées pour eux font qu'il est quasiment impossible d'enregistrer ces vulnérabilités au jour le jour et d'y remédier. Cette tendance s'observe dans la variété des applications et systèmes d'exploitation vulnérables (voir les illustrations 4 et 5).

Illustration 4 : Les applications les plus ciblées[8]

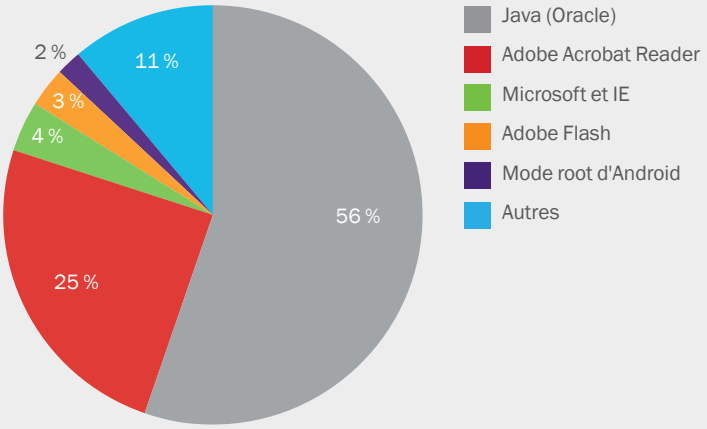


Illustration 5 : Les 10 principales vulnérabilités logicielles, premier trimestre 2012[9]

Classement	Application vulnérable	% d'utilisateurs vulnérables	Évaluation
1	Oracle Java (plusieurs vulnérabilités)	35 %	Très critique
2	Oracle Java (trois vulnérabilités)	21,7 %	Extrêmement critique
3	Adobe Flash Player (plusieurs vulnérabilités)	19 %	Très critique
4	Adobe Flash Player (plusieurs vulnérabilités)	18,8 %	Très critique
5	Adobe Reader/Acrobat (plusieurs vulnérabilités)	14,7 %	Extrêmement critique
6	Apple QuickTime (plusieurs vulnérabilités)	13,8 %	Très critique
7	Apple iTunes (plusieurs vulnérabilités)	11,7 %	Très critique
8	Winamp (traitement des fichiers AVI/IT)	10,9 %	Très critique
9	Adobe Shockwave Player (plusieurs vulnérabilités)	10,8 %	Très critique
10	Adobe Flash Player (plusieurs vulnérabilités)	9,7 %	Extrêmement critique

8 Source : https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#4
9 Source : https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#14

Menaces :
une nouvelle ère de sophistication

Lutte contre les fuites d'informations : la montée en puissance du chiffrement de données

- 15 % des entreprises ont subi une perte de données suite au vol de périphériques mobiles [11]
- Les programmes malveillants et le courrier indésirable restent les causes majeures de perte de données [11]
- Le chiffrement de données se classe à la deuxième place dans la liste des domaines que la plupart des entreprises souhaiteraient améliorer.[11]

3.3 La dimension mobile

La mobilité ajoute une nouvelle dimension aux risques. Aujourd'hui, iOS et OS X d'Apple ainsi que les diverses variantes Google de systèmes d'exploitation Android sont aussi prolifiques que Windows.

Les cybercriminels ont une longueur d'avance dans l'exploitation des risques liés à la mobilité. Au deuxième trimestre 2012, le nombre de chevaux de Troie visant la plate-forme Android a presque triplé par rapport au premier trimestre 2012 (voir l'illustration 6).

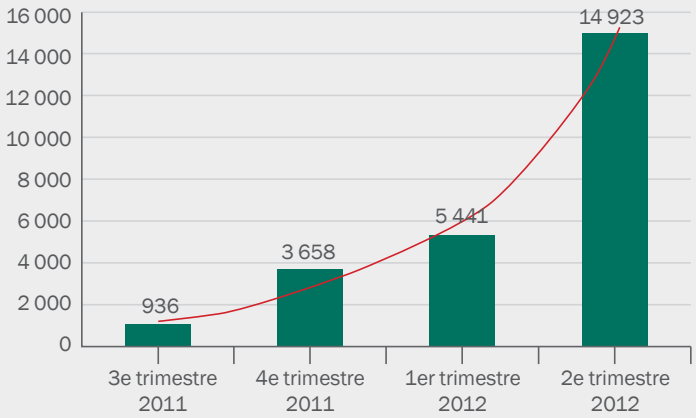


Illustration 6 : Le nombre de programmes malveillants ciblant le système d'exploitation Android[10]

Des chiffres appelés à augmenter puisque la facilité avec laquelle les données mobiles d'un professionnel peuvent être obtenues ou interceptées fait de la mobilité un nouveau terrain à exploiter par la cybercriminalité.

L'enquête 2012 de Kaspersky sur les risques informatiques mondiaux a mis en évidence la tendance consistant à apporter son propre appareil au bureau (BYOD) et elle montre que de plus en plus d'entreprises autorisent les propriétaires de ces appareils à accéder aux données et réseaux d'entreprise, sans mesures de sécurité supplémentaires. Cette approche étonnamment laxiste s'explique par plusieurs facteurs, mais principalement la rapidité d'adoption de ces appareils et le fait que les types de périphériques différents et les versions de systèmes d'exploitation sont tout simplement trop nombreux pour être gérés par une équipe informatique qui manque de ressources.

La connectivité sans fil, les services cloud et les applications de synchronisation de fichiers font de ces dispositifs des cibles très prisées pour le vol physique.

Les voleurs et les pirates ayant accès à des périphériques mobiles volés compromettent leur sécurité pour voler des données sensibles ou les utilisent pour pénétrer sur les réseaux d'entreprise. Le préjudice financier direct lié à la perte et au vol de périphériques est estimé à 7 millions de dollars par an[12] ; les coûts indirects des piratages associés restent inconnus.

3.4 Médias sociaux : recul des restrictions malgré l'augmentation des risques

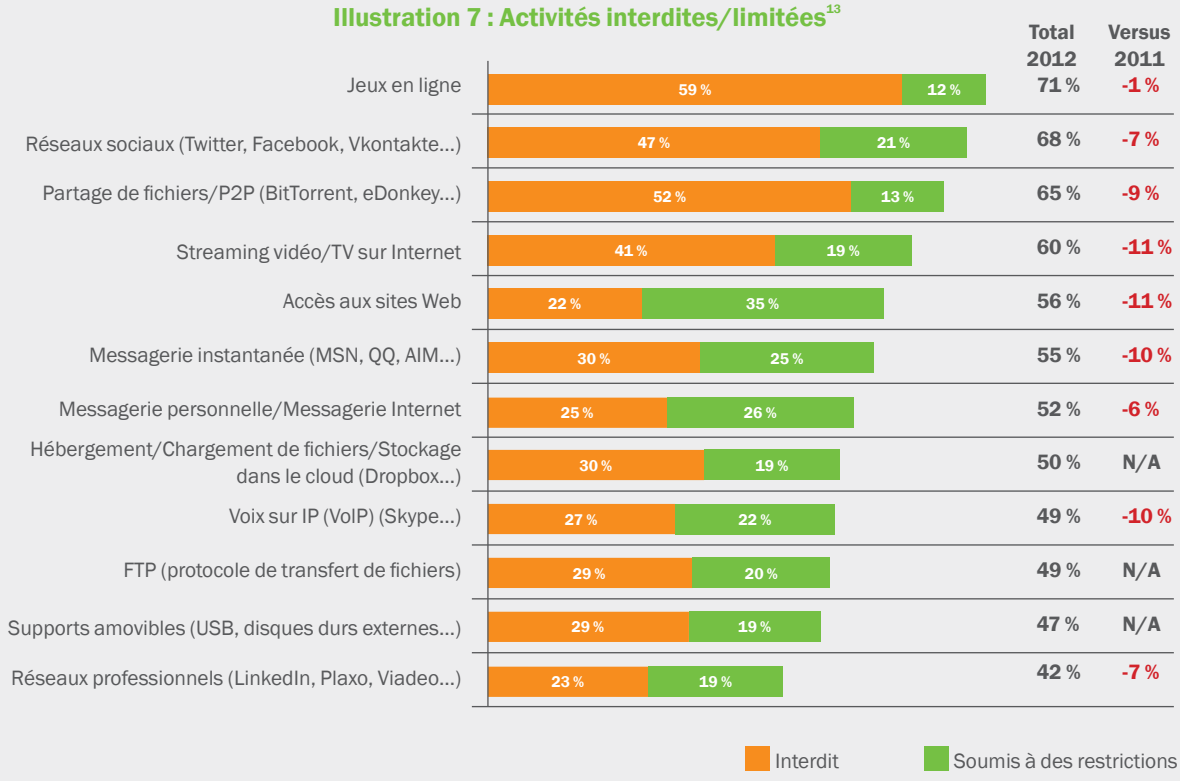
Les administrateurs informatiques soulignent à juste titre que les risques les plus importants en matière de sécurité ne sont pas le fait des technologies elles-mêmes, mais des individus. L'omniprésence des médias sociaux et du Web et le souhait des individus d'être connectés en permanence compliquent considérablement la tâche des équipes informatiques chargées de gérer les risques liés à la sécurité.

10 Source : rapport securelist.com du 2e trimestre 2012 : http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012
11 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux
12 Source : https://www.lookout.com/resources/reports/mobile-lost-and-found/billion-dollar-phone-bill

Le sujet le plus épineux est l'usage des médias sociaux. Considérée comme l'une des plus grandes menaces pour la sécurité informatique, cette activité figure au deuxième rang des pratiques les plus étroitement contrôlées, seules un peu plus de la moitié des entreprises l'interdisant en bloc (voir l'illustration 7). Les restrictions autour de l'usage des médias sociaux et du Web sont en recul, bien qu'il soit difficile d'en déterminer la raison : l'informatique, grand perdant de la bataille, ou l'intérêt commercial incontournable de ces usages.

Comme l'explique David Emm, Senior Regional Researcher chez Kaspersky : « *Interdire l'utilisation des réseaux sociaux dans toute l'entreprise reviendrait à essayer d'inverser la tendance : il est bien plus judicieux de réfléchir à la manière de mieux la gérer.* »[14]

Illustration 7 : Activités interdites/limitées[13]



La conclusion alarmante est cependant que les entreprises n'ont pas cherché à résoudre cet aspect des choses. Gérer l'utilisation des médias sociaux et se protéger d'un usage sans entrave du Web constitueront une facette majeure de l'entreprise bien protégée du futur. Les « risques inhérents » des médias sociaux sont en réalité moins en cause que le fait que les utilisateurs cliquent sur les publiciels et sondages qui y sont incorporés et surtout moins que la propension générale au partage qui semble s'être installée. Considérés par beaucoup comme des activités sûres et légitimes, les sites FTP, l'hébergement de fichiers et les chargements vers des serveurs ouvrent la porte à de nombreux risques importants en matière de sécurité informatique.

Il incombe aux équipes informatiques de prendre conscience de l'étendue et de la gravité de ces nouveaux dangers ainsi que de leur prédominance au sein de la communauté des utilisateurs finaux. C'est seulement à cette condition que les entreprises de toutes tailles pourront réévaluer de manière objective leur approche et leur dispositif de sécurité actuels.

13 Source : enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial
14 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux

Simplifier la situation à l'aide d'une seule et même plate-forme

4.0

Plusieurs angles de vue, autant de solutions : la protection de l'entreprise est un sujet complexe

- 44 % des entreprises chiffrent désormais leurs données sensibles
- 33 % des entreprises autorisent un accès « non contrôlé » au réseau via les smartphones[15]

4.1 Pourquoi l'industrie de la sécurité informatique n'a fait que compliquer les choses

Jusqu'ici, l'industrie de la sécurité informatique n'a pas cherché à rendre la tâche plus aisée aux entreprises. Seules des solutions ponctuelles ont jusqu'à présent été proposées en réponse à la prolifération de technologies différentes. Loin d'être inhabituel en soi, ce phénomène est simplement symptomatique d'un marché en phase de maturation et de l'évolution des technologies.

Dans les entreprises ne disposant pas d'une équipe de sécurité informatique dédiée, l'étude de l'offre du marché peut être une expérience déroutante et frustrante pour les services informatiques en charge de multiples tâches. Rechercher, évaluer et acquérir les produits dont l'entreprise a besoin est une tâche des plus complexes.

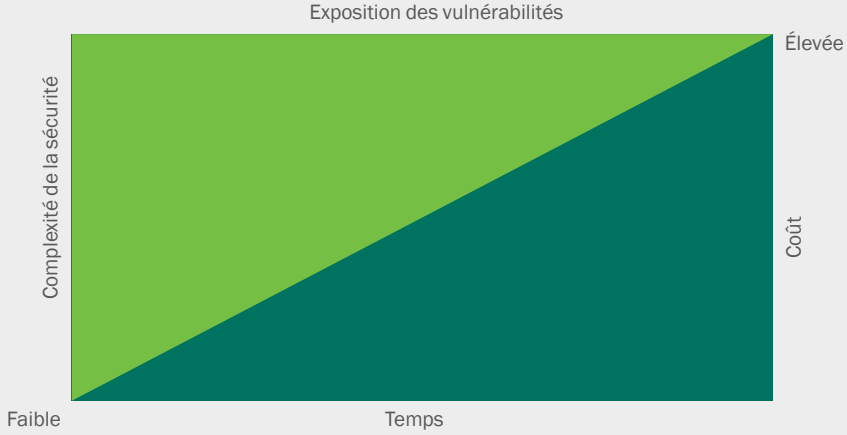
Les entreprises utilisent souvent un programme traditionnel de protection contre les programmes malveillants pour leurs besoins essentiels de sécurité des terminaux. Elles y ajoutent parfois un chiffrement des e-mails et des systèmes de partage de fichiers. Si leur personnel comprend des utilisateurs mobiles, elles peuvent investir dans une technologie de gestion des périphériques mobiles pour contrôler et contenir le flux entrant d'appareils personnels et d'appareils parrainés par l'entreprise. Enfin, elles mettent en place une gestion des correctifs, pour suivre et déployer les corrections de logiciels à travers leurs environnements d'exploitation dans le but d'éviter que les applications ne deviennent des failles de sécurité.

Les entreprises ont donc déjà réalisé des investissements importants mais font alors face à un défi beaucoup plus grand.

Les systèmes de sécurité ne communiquent tout simplement pas entre eux. Chaque fois qu'un administrateur de systèmes exécute un rapport, met en œuvre un changement, réagit à une alerte ou met à jour un logiciel, il doit utiliser une console d'administration différente pour chaque application spécifique. Cette coordination manuelle de technologies soi-disant « connectées » se révèle inefficace et très gourmande en temps (voir l'illustration 8). Plus que tout, elle va à l'encontre d'une sécurité efficace.

Par exemple, en supposant que vous disposiez de cinq applications de sécurité différentes et que cinq minutes soient nécessaires à l'exécution d'une seule fonction sur chaque plate-forme afin d'entreprendre une action de sécurité coordonnée, la mise en œuvre du changement prendra un total de 25 minutes. Ajoutez à cela les efforts nécessaires pour s'assurer que le changement a été correctement déployé, étant donné que les mécanismes de génération de rapports varient entre les applications. Le résultat final n'est autre qu'un administrateur de la sécurité contraint de consacrer de longues heures à passer au crible rapports et écrans pour exécuter une fonction qui devrait être relativement automatique.

Illustration 8 : La complexité est le pire ennemi de l'efficacité en sécurité informatique. Plus les technologies de sécurité sont complexes, plus la mise en œuvre d'un changement prend du temps, plus le coût de la sécurité est élevé et plus faible est le retour sur investissement des dépenses de sécurité.[16]



15 Source : enquête 2012 de Kaspersky sur les risques informatiques au niveau mondial
16 Source : 2112 Group, « Complexity is the enemy of security », octobre 2012.

« Tout comme les lacunes en termes de connaissances et de préparation, il existe également dans bon nombre d'organisations d'importantes failles au niveau opérationnel, avec différentes solutions et politiques de sécurité appliquées à différents groupes d'utilisateurs et périphériques. Chacune de ces lacunes constitue une vulnérabilité potentielle ; les organisations doivent adopter une approche globale et étudier des solutions de contrôle intégrées. »
Chris Christiansen
IDC – VP Security Products and Services[17]

Si le terme « intégration » est galvaudé en informatique, il désigne néanmoins un facteur déterminant pour améliorer tout dispositif de sécurité. Il est impossible, pour des équipes aux ressources limitées, de gérer plusieurs systèmes, de surveiller plusieurs tableaux de bord, puis de prendre des mesures correctives.

Or, la rapidité d'identification et de réaction est particulièrement importante en matière de sécurité informatique ; dans un environnement réseau normal, plus les applications restent longtemps dépourvues de correctifs, plus leur potentiel de vulnérabilité s'accroît. Prenez ce scénario et étendez-le à l'environnement complexe actuel, composé de périphériques mobiles, de machines virtuelles et d'appareils détenus par les employés. La facilité et la rapidité de mise en œuvre des changements fait partie des composantes essentielles d'une approche efficace.

La raison pour laquelle le terme d'« intégration » est aussi problématique dans ce contexte est que de nombreuses approches « consolidées » ont été créées simplement en mettant bout à bout diverses solutions ponctuelles. Cette manière de faire n'est pas un problème en soi, les technologies « fonctionneront » certainement bien ensemble ; mais elles ne permettront pas d'obtenir un processus fluide et harmonieux. Plus important encore, cette approche n'est pas idéale en termes de rapidité : comprendre les différentes interfaces et s'assurer que les politiques sont appliquées de manière appropriée et cohérente sur différentes technologies reliées les unes aux autres nécessitent des efforts manuels non négligeables.

Le temps est une ressource précieuse dont les équipes informatiques surchargées manquent déjà. Ce que ces équipes attendent ? Une seule manière de réaliser plusieurs tâches dans toutes sortes d'environnements.

17 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux

Comment protéger ce qu'on ne voit pas ? Une administration simplifiée vous apporte une nouvelle visibilité

5.0

5.1 L'obstacle des coûts et des ressources
Alors que les entreprises adoptent des technologies diverses et nombreuses, adhèrent à la mobilité et à la collaboration et deviennent dépendantes d'opérations basées sur les données pour des critères d'efficacité tels que la continuité et la productivité, il est fondamental qu'elles améliorent leur dispositif de sécurité et qu'elles réduisent les risques ainsi que l'exposition aux pirates et aux programmes malveillants. Malheureusement, les besoins de sécurité ne sont pas proportionnels aux ressources et l'augmentation des dépenses informatiques n'est pas nécessairement synonyme d'accroissement du personnel et de l'expertise.

Les spécialistes de la sécurité informatique cherchent à créer et commercialiser des applications et outils offrant une plus grande interopérabilité et une meilleure intégration. Aujourd'hui, les grandes entreprises atteignent leurs objectifs grâce à des systèmes personnalisés qui compilent et standardisent la génération de rapports. Mais cette approche coûteuse requiert des ressources internes spécialisées pour la gestion de ces systèmes, ce qui en fait une option rarement envisageable pour la majorité des petites entreprises.

5.2 Briser le moule : identifier, contrôler et protéger tous les terminaux à partir d'un point unique
La nouvelle approche commence avec une seule et même plate-forme, le fameux point de contrôle unique qui offre aux administrateurs informatiques une vue centralisée et la visibilité nécessaire pour protéger leur entreprise et ses données en ayant toutes les informations en main.

La visibilité mène au contrôle et le contrôle à la protection.

Par conséquent, pour toutes les entreprises à l'exception des plus grandes, les solutions choisies doivent éviter le recours à de multiples systèmes d'administration, ne pas nécessiter d'intégration des systèmes et pouvoir être administrées par des non-spécialistes de la sécurité informatique. Ces solutions doivent malgré tout fournir un moyen transparent d'identifier, contrôler et protéger tous les terminaux contenant des données d'entreprise, qu'elles se trouvent sur des ordinateurs de bureau, des machines virtuelles, des tablettes, des smartphones ou même les propres appareils des employés.

Au cœur de ce système doit se trouver une console d'administration unique et cohérente. Les outils de sécurité sont alors accessibles et contrôlables à partir d'un tableau de bord unique, avec une manière homogène de configurer, délivrer et gérer les politiques et les paramètres de sécurité à travers l'entreprise.

Conclusion

6.0

Kaspersky Endpoint Security for Business inclut :

- Protection contre les programmes malveillants
- Chiffrement des données
- Sécurité et gestion de flotte mobile
- Contrôle des applications, des périphériques et du Web
- Gestion des systèmes, notamment gestion des correctifs

Kaspersky s'est aperçu que, pour la plupart des entreprises, sécuriser et gérer l'ensemble des dispositifs informatiques est devenu un travail considérable de plus en plus frustrant. Il apparaît clairement que résoudre le problème de la complexité nécessite impérativement une approche unique et consolidée de la sécurité informatique. Les besoins et problématiques abordés dans cette publication ont conduit Kaspersky à développer une nouvelle approche baptisée Kaspersky Endpoint Security for Business.

Kaspersky Endpoint Security for Business est fondamentalement différent de tous les autres produits actuellement proposés sur le marché, dans la mesure où cette plate-forme a été développée de A à Z. En d'autres termes, il s'agit d'une plate-forme de sécurité informatique unique et non d'une multitude de logiciels reliés les uns aux autres.

La maintenance de votre dispositif de sécurité global en est ainsi largement facilitée, les politiques pouvant être définies une seule fois, puis déployées d'un simple clic sur un bouton vers toutes sortes de terminaux et d'environnements.

Kaspersky Endpoint Security for Business fournit une plate-forme complète, entièrement intégrée qui vous offre la meilleure protection au monde contre les programmes malveillants, des outils solides de contrôle des applications, plus des fonctions de gestion des systèmes, de chiffrement des données et de gestion des périphériques mobiles, tous gérés à partir d'une seule console. Pour protéger vos données, gérer vos applications et vous donner la possibilité d'identifier, contrôler et sécuriser l'ensemble des périphériques, qu'ils soient physiques, virtuels ou mobiles, professionnels ou personnels.

De cette manière, les entreprises peuvent enfin atteindre de hauts niveaux de protection à l'échelle d'un environnement informatique complexe et évoluant fréquemment, mais avec des besoins de formation et d'expertise réduits au minimum. Ce qui était autrefois considéré comme des technologies complexes, coûteuses et difficiles à gérer devient une réalité accessible à toutes les entreprises, quelles que soient leur taille ou leurs ressources.

Identifier, contrôler, protéger. Avec Kaspersky Endpoint Security for Business, maintenant c'est possible.

À propos de Kaspersky

Kaspersky Lab est le plus grand fournisseur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux fournisseurs au monde de solutions de sécurité pour utilisateurs de terminaux. Tout au long de ses quinze ans d'existence, Kaspersky Lab a fait figure d'innovateur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux consommateurs, PME et grandes entreprises. La société est actuellement présente dans près de 200 pays et territoires à travers le monde, où elle apporte une protection à plus de 300 millions d'utilisateurs.

Plus d'informations sur : www.kaspersky.fr/business