Vos concurrents s'inquiètent du comportement de leurs employés, et vous ?

Surmontez vos craintes en matière de sécurité face à la généralisation du télétravail

kaspersky BRING ON THE FUTURE

Introduction

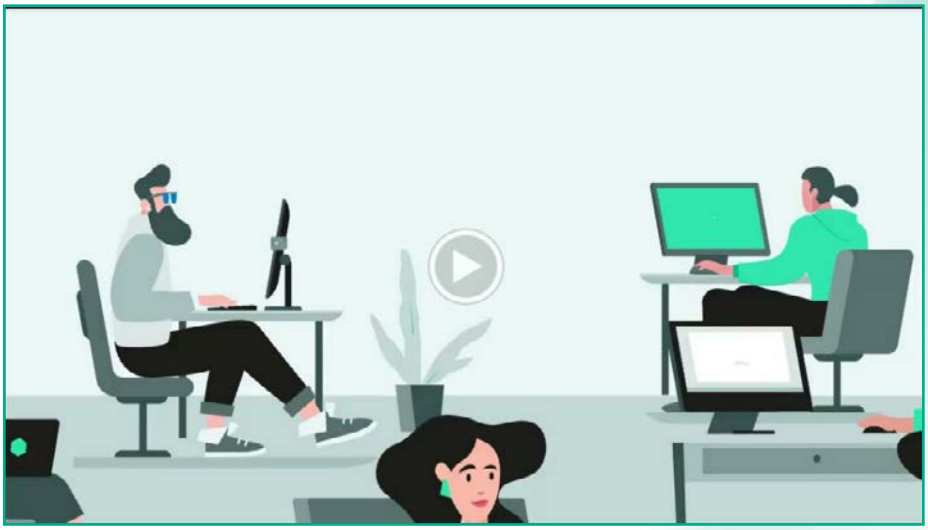
Une mauvaise hygiène en matière de sécurité représente un véritable casse-tête pour les dirigeants d'entreprises et les équipes de sécurité. Le développement du télétravail post-pandémie a étendu la surface d'attaque de presque toutes les entreprises, et il devient de plus en plus difficile de suivre le comportement des employés. Les périmètres physiques se dissolvent, les stratégies de sécurité échouent et le Shadow IT devient la norme.

Le réseau domestique est également devenu le réseau professionnel, mais la sécurité n'a pas rattrapé son retard. Les entreprises déploient des solutions qui ne les protègent pas de la naïveté des employés, dans la mesure où les formations cloisonnées, la faible visibilité des données et les stratégies peu efficaces sont monnaie courante.

Le coût de la négligence est élevé : les violations de données où le travail à distance est en cause coûtent environ un million de dollars de plus[1] que les violations où le travail à distance ne joue aucun rôle. Or, restreindre les possibilités de travail à distance n'est pas la solution. Les talents de tous les départements demandent maintenant à travailler de manière flexible (pas seulement ceux qui disposent de compétences techniques). Par conséquent, imposer un **lieu de travail** aux employés revient à limiter le choix des personnes **avec lesquelles** vous travaillez.

Ce livre blanc se penche sur les menaces liées à l'hygiène en matière de sécurité en vous présentant les points à surveiller et, enfin, en décrivant comment retrouver une visibilité organisationnelle. Prenons l'exemple de votre entreprise. Savez-vous à quand remonte la dernière fois où une clé USB pirate a été branchée sur un appareil de votre entreprise ? Si des mots de passe sont partagés avec des tiers « de confiance » ? Si des informations personnellement identifiables (PII) sont en circulation dans le cloud public ?

Autant de scénarios qui menacent votre sécurité et votre solde bancaire. Nous avons la solution.



Comment le réseau domestique est devenu le réseau professionnel

Le travail à distance était autrefois un territoire réservé aux employés dont les compétences étaient si rares qu'ils pouvaient exiger de travailler de n'importe où. Les postes vacants dans le cloud, par exemple, ont augmenté de 94 %[2] entre 2017 et 2020, ce qui signifie que les architectes du cloud (qui étaient déjà en nombre insuffisant[3]) avaient une multitude de débouchés. Les entreprises qui proposent un travail flexible ont dominé le recrutement de ces talents.

Cependant, notre façon de travailler a rattrapé son retard. Une étude menée par McKinsey[4] montre que 58 % des Américains ont la possibilité de travailler à domicile au moins une fois par semaine, tandis qu'un tiers peut le faire à temps plein. Cette évolution concerne les travailleurs de tous les domaines, même les « cols bleus », qui travaillaient autrefois exclusivement sur place.

Avant la pandémie, seuls 6 % d'entre nous[5] travaillaient principalement à domicile. Désormais, le réseau domestique est devenu le réseau professionnel, ce que trois quarts des PDG ont prédit en 2020[6] en admettant la nécessité de réduire les espaces de bureau. Ce que ces PDG n'avaient peut-être pas prévu, c'est le risque de sécurité que cette évolution introduirait ainsi que son incidence sur leurs propres activités. PWC a constaté[7] qu'en 2022, les PDG étaient plus inquiets des conséquences d'une cyberattaque que de toute autre chose, même des risques pour la santé. Plusieurs facteurs ont contribué à cette préoccupation, notamment :

- La couverture apocalyptique des cyberattaques par les médias
- Le coût et la fréquence des violations qui font l'objet d'une grande couverture médiatique
- L'expansion rapide des surfaces d'attaque et la complexité des réglementations

Ce dernier point est l'un de ceux sur lesquels un responsable de la sécurité bien préparé (pensez au financement, au personnel et à l'outillage) peut agir, ce qui peut contribuer à apaiser les craintes d'un PDG. Or, la plupart des responsables de la sécurité n'ont pas la visibilité nécessaire pour prospérer dans un environnement qui privilégie le travail à distance, ce qui favorise le stress, la désaffection et même l'épuisement professionnel.

Les risques posés par le télétravail

La pandémie de Covid-19 est certes devenue moins pesante dans de nombreuses régions, mais les organisations sont désormais confrontées à la menace que constituent les cyberattaques. IBM et Morning Consult ont constaté[8] que les employés qui travaillent à distance pour la première fois représentent un risque pour la sécurité, car ils sont généralement trop confiants et mal préparés. La vulnérabilité des organisations s'en est trouvée décuplée, au point que les piratages et les violations de données sont désormais très probables. Cependant, malgré ce que disent les prophètes de malheur sur LinkedIn, elles **ne sont pas** inévitables. Les risques peuvent être atténués – si vous comprenez les facteurs qui entrent en jeu.

Dissolution des périmètres

Le périmètre des réseaux d'entreprise s'est dissous en raison des politiques BYOD, et les contraintes qui protégeaient autrefois les data centers nsur site et les systèmes d'information des entreprises ne sont plus efficaces. Les données sont désormais stockées dans le cloud afin de permettre le travail à distance : ainsi, les employés partagent des informations privées avec des tiers.

Mauvaise hygiène en matière de sécurité

Une mauvaise hygiène de l'utilisateur final en matière de sécurité correspond à un manque général de connaissances appropriées dans ce domaine, comme l'utilisation de mots de passe faibles (prendre de mauvaises mesures), le fait de ne pas détruire des documents confidentiels (oublier de prendre des mesures) et le fait d'ignorer les stratégies de l'entreprise (refuser de prendre des mesures). Ce type d'erreur humaine est à l'origine de 82 % des violations de données[9] et peut être exploité par des acteurs malveillants peu qualifiés.

Shadow IT

Lorsque les employés utilisent des services et des programmes à l'insu de leur département informatique, vous vous retrouvez face à un comportement appelé Shadow IT, et celui-ci pose des problèmes. Ce comportement se manifeste généralement lorsqu'un employé bien intentionné utilise un outil privilégié, mais non approuvé, pour accomplir ses tâches. Cette approche peut améliorer les processus, mais elle est souvent source de stress pour les services informatiques surchargés et, surtout, elle comporte des risques.

Les services en ligne inconnus peuvent être vulnérables, voire malveillants, et les employés n'ont souvent aucune idée si l'application qu'ils ont installée a été développée de manière sécurisée. Certains employés peuvent même ne pas s'en soucier. Un autre problème est que ceux qui **devraient** être au courant de ce qui se passe (les services de sécurité et/ou d'informatique) sont ceux qui en savent le moins. L'application ou le service malveillant n'est pas pris en compte dans les modèles de menaces, les décisions de planification, etc., et il en résulte[10] un risque plus important. Ce qui inclut :

- Fuites de données
- Vulnérabilités non corrigées
- Droits d'accès non gérés
- Violations des réglementations
- Budget gaspillé

Le risque diminue si les employés présentent chaque nouvelle application ou service qu'ils utilisent au service de sécurité/IT, mais cette possibilité est de moins en moins probable dans un monde qui privilégie le télétravail, où la vie professionnelle et la vie privée ont fusionné. Il est donc crucial de contrôler le Shadow IT, et il est possible d'y parvenir sans effort, comme vous le constaterez dans quelques instants.

Stress

Il y a plusieurs avantages à travailler à distance, comme le temps économisé sur les trajets et la prise d'appels en chemise de nuit, mais 54 % des employés[11] se retrouvent en fait avec plus de travail. Cette situation peut provoquer du stress, ce qui a une influence sur le comportement de l'utilisateur final, car les gens sont plus susceptibles de commettre des erreurs lorsqu'ils sont sous pression. Selon les résultats de Harvard Business Review, une violation de la politique de sécurité sur cinq[12] est désormais justifiée par la volonté d'aider un collègue. Pour faire face à l'augmentation des défis, l'altruisme se développe, ce qui, bien que salutaire pour les relations amicales, est néfaste pour la sécurité.

Le stress peut également entraîner la fatigue et réduire la vigilance. Les pirates informatiques le savent. C'est pourquoi ils ont intensifié leurs tentatives de phishing[13] en pleine pandémie, alors que l'anxiété était à son comble. Il n'existe pas de solution miracle pour atténuer le stress des employés, mais vous pouvez fournir à vos collaborateurs le filet de sécurité dont ils ont besoin pour pouvoir se tromper sans crainte.

Gestion actuelle de l'hygiène en matière de sécurité

La formation de sensibilisation à la sécurité

La formation de sensibilisation à la sécurité consiste, en pratique, à adapter les employés à leurs fonctions. Vous devez faire en sorte que vos employés comprennent leur rôle dans la protection de l'entreprise. Vous devez donc leur expliquer que la sécurité n'est plus l'apanage de quelques privilégiés, mais qu'elle est devenue le problème de tous. Vous mobilisez les membres de chaque département avec une formation ludique (ou un PowerPoint si vous êtes cruel) et leur donnez carte blanche en sachant qu'ils comprennent ce qu'il faut faire, ou ne pas faire.

C'est la théorie, en tout cas.

La réalité est que si la plupart des entreprises[14] disposent d'un programme de sensibilisation à la sécurité, seules 43 % le déploient dans toute l'entreprise. Une entreprise est aussi forte que son maillon le plus faible, donc si cette formation n'est pas dispensée à chaque employé, elle n'est probablement pas efficace. Même une formation régulière et de qualité peut ne pas suffire. Les gens savent qu'ils devraient faire plus d'exercice, mais cela ne signifie pas pour autant qu'ils le feront. C'est la nature humaine.

Stratégies

Vous pourriez penser que les stratégies sont synonymes de conformité, mais au-delà des contraintes physiques du bureau, avec moins de témoins, ce n'est pas toujours le cas. Harvard Business Review a constaté dans une enquête que deux tiers[12] des employés travaillant à distance n'ont pas respecté les stratégies de cybersécurité au moins une fois, et que les gens sont beaucoup plus susceptibles d'enfreindre les protocoles de sécurité lorsqu'ils sont stressés (comme nous l'avons mis en évidence précédemment). Et le stress – qu'il s'agisse d'un enfant qui se comporte mal, du syndrome de l'imposteur ou des exigences liées au respect des stratégies proprement dites – réduit la tolérance des employés à l'égard des règles.

La révision des stratégies de sécurité est une mesure populaire que les entreprises adoptent pour atténuer le risque d'une violation des données, mais près de la moitié[11] des petites et moyennes entreprises (PME) ont subi une violation de la sécurité informatique. Les stratégies seules ne suffisent pas.

Protection des terminaux

Pour une sécurité efficace du télétravail, nous vous conseillons d'investir dans une suite complète de protection des terminaux (EPP) pour votre entreprise. Cette mesure vous permettra de détecter les programmes malveillants sur une machine infectée et d'y répondre. La protection des terminaux comprend non seulement la détection antivirus, mais aussi des pare-feu, des logiciels contre les programmes malveillants, la prévention des pertes de données et bien plus encore.

Détection et réponse au niveau des terminaux (EDR)

Les solutions de sécurité qui intègrent l'EDR vous aident à visualiser les chemins d'accès des attaques, et sont donc encore plus efficaces. Par exemple, un fichier malveillant en apparence inactif pourrait se servir d'outils légitimes pour générer des processus enfants, se connecter à des serveurs de commande et de contrôle, et créer des fichiers. Ceux-ci seraient bloqués par la solution EPP, mais l'EDR vous présenterait la **cause profonde** pour vous aider à comprendre l'origine et la portée de l'attaque, en s'assurant que des indicateurs de compromission (IoC) similaires ont été détectés sur les machines voisines. Et comme l'EDR intègre une réponse automatisée, les machines compromises seraient isolées du réseau et les éléments malveillants seraient mis en quarantaine. Le chargement des IoC dans un système EDR peut même vous aider à empêcher les attaques avant qu'elles ne commencent – et ce n'est là qu'une seule des fonctionnalités de Kaspersky Endpoint Security Cloud.

Comment Kaspersky Endpoint Security Cloud protège votre entreprise

Visibilité totale

Si vos employés utilisent des services cloud non professionnels, il existe un risque de fuite de données. Kaspersky Endpoint Security Cloud vous permet de connaître les ressources que vos employés utilisent afin que vous puissiez décider des mesures à prendre. Cela ne signifie pas qu'il faut suivre le moindre mouvement des utilisateurs (nous laissons cela à Big Brother), mais qu'il convient de surveiller les outils non professionnels utilisés afin de réduire votre surface d'attaque. Les contrats d'entreprise, par exemple, passent-ils par des services cloud qui convertissent les documents DOCX en fichiers PDF ? Notre service OneDrive d'entreprise peut facilement résoudre ce problème.

Kaspersky Endpoint Security Cloud vous aidera à réduire le nombre de services informatiques dans le cloud non contrôlés sur le réseau de l'entreprise, par exemple :

- Partage de fichiers
- Messageries Web
- Réseaux sociaux
- Messenger

Sérénité totale

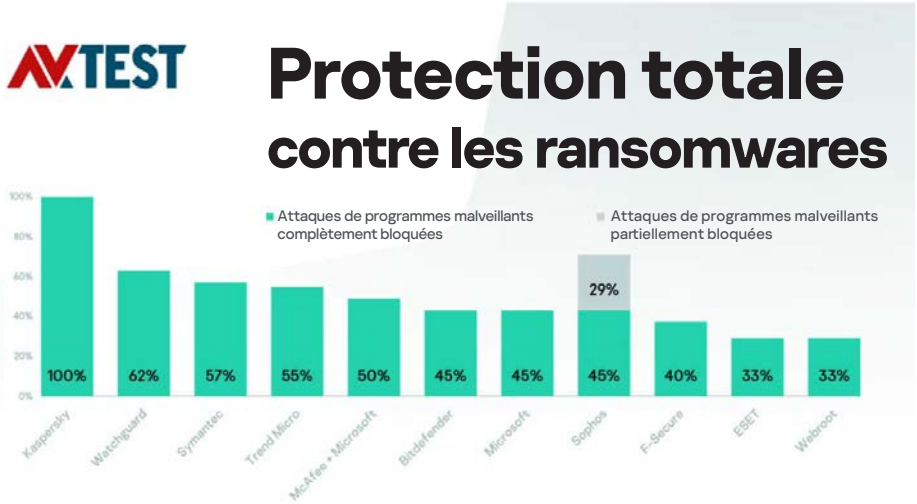
Si l'un de vos employés trouve une clé USB dans un bus et décide de la brancher par curiosité (un exemple parfait de mauvaise pratique en matière de sécurité), vous pourriez être confronté à de gros problèmes. Cependant, avec Kaspersky Endpoint Security Cloud, qui peut interdire l'utilisation d'appareils externes et exécuter des analyses automatisées, les erreurs innocentes ne sont plus qu'un souvenir.

Nous veillons à ce que votre protection soit toujours à jour, et en cas d'attaque, vous pouvez voir exactement ce qui se passe, déterminer la cause et y remédier rapidement.

Des tests indépendants prouvent également que Kaspersky Endpoint Security Cloud a une longueur d'avance dans la qualité de sa protection. Entre 2013 et 2021, ce sont **518 premières places** qui ont été décernées à nos produits, soit plus qu'à tout autre éditeur. Mieux encore, nous sommes le seul fournisseur à bloquer 100 % des attaques de ransomwares[15].

Avantage pour les clients :

Kaspersky Endpoint Security Cloud fournit tout ce dont vous avez besoin pour protéger vos ordinateurs de bureau et serveurs de fichiers Windows, vos appareils Mac OS, vos appareils mobiles iOS et Android ainsi que Microsoft Office 365. Notre offre premium, Kaspersky Endpoint Security Cloud Pro, est environ **30 % moins chère que la solution équivalente de Microsoft** et couvre 1 000 terminaux (il n'est donc pas nécessaire de procéder à des mises à niveau coûteuses).



Sécurisez vos données avec Kaspersky Endpoint Security Cloud

Les préoccupations liées à l'hygiène en matière de sécurité ne sont pas une raison pour renoncer aux modes de travail à distance et hybride. Selon le cabinet McKinsey[4], le travail flexible est le troisième facteur de motivation des demandeurs d'emploi, devant l'assurance maladie et même les congés payés. Les meilleurs talents, y compris les innovateurs numériques difficiles à recruter, l'exigent.

Kaspersky Endpoint Security Cloud propose tout ce dont vous avez besoin pour vaincre facilement vos craintes concernant l'hygiène en matière de sécurité.

Protégez vos employés travaillant à distance, où qu'ils soient

- Soyez partout et assurez votre protection partout grâce à la console cloud, quel que soit l'endroit où se trouvent vos employés ou les appareils qu'ils utilisent.
- Activez le chiffrement à distance pour garantir la sécurité des données de votre entreprise, même en cas de perte ou de vol d'un appareil.
- Assurez-vous que les appareils mobiles hors de votre champ de vision restent sécurisés grâce à un riche ensemble de fonctions de gestion et de chiffrement.

Reprenez le contrôle du cloud

- Découvrez le Shadow IT, gardez le contrôle de votre infrastructure, limitez les services cloud non autorisés ou certains utilisateurs de votre réseau, et évitez les atteintes à la protection des données.
- Activez une coopération et une communication sécurisées dans Microsoft Office 365 grâce à la protection incluse pour ses principales applications.
- Garantissez votre conformité grâce à l'audit continu de vos données dans le cloud. Identifiez les informations confidentielles liées à des informations personnellement identifiables (PII) et à des données de paiement, et découvrez si elles sont partagées dans les services Microsoft.

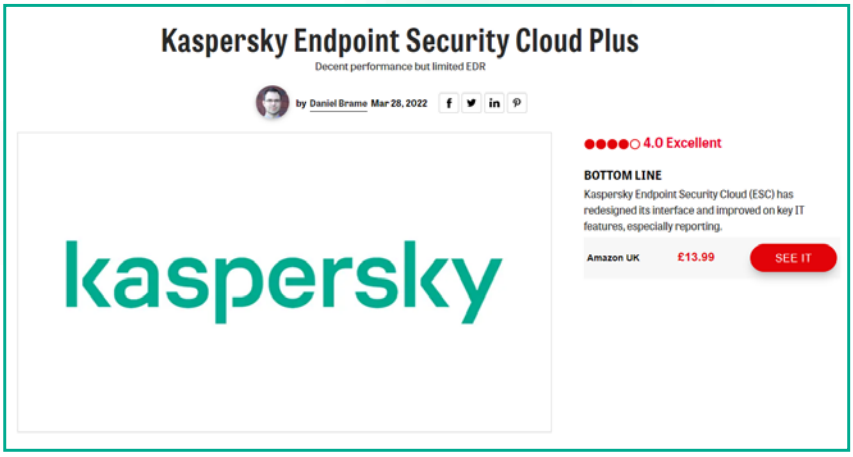
AV-TEST

Informations d'identification personnelles
Protection : données sensibles
Test de découverte.

En savoir plus

Protégez votre entreprise rapidement

- Installez facilement la solution en envoyant une invitation pour mettre en place immédiatement une protection par navigateur (aucun serveur requis). Grâce à un assistant d'utilisation des produits, vous n'avez plus besoin de formation.
- Passez à la protection supérieure en quelques clics, afin de pouvoir augmenter le nombre d'appareils à mesure que votre entreprise se développe.
- Détendez-vous en sachant que nous gardons tout sous contrôle – aucun support matériel ou logiciel encombrant n'est nécessaire.



Conclusions

Les violations où le télétravail entre en jeu coûtent environ un million de dollars[1] de plus que les violations où il ne joue aucun rôle (bien que ce montant soit proportionnellement moins élevé pour les PME), mais cela ne signifie pas que vous devez reconsidérer votre mode de fonctionnement. Bien au contraire. Le travail à distance est une réalité, et ce, pour une bonne raison : nous sommes nombreux à en tirer profit en augmentant notre productivité, en améliorant notre accès aux talents et en réduisant nos frais généraux.

Le coût de Kaspersky Endpoint Security Cloud est négligeable par rapport à celui d'une violation. Nous vous aiderons à vous protéger partout afin que vous puissiez continuer à développer votre personnel à distance en toute confiance – maintenant et à l'avenir. Et avec trois versions disponibles, proposés par appareil, vous ne payez que pour ce dont vous avez besoin.

Il est temps de se tourner vers l'avenir.
Obtenez votre essai gratuit de 30 jours dès aujourd'hui.

À propos de Kaspersky

Kaspersky protège plus de 400 millions d'utilisateurs et 240 000 entreprises. Est. 1997.

Nous sommes une entreprise internationale privée dont la société holding est établie au Royaume-Uni.

Nous transformons nos renseignements de sécurité de pointe en une protection réelle pour nos clients. Nous vous donnons les moyens d'utiliser les technologies au quotidien et au travail en toute sécurité et en toute confiance.

Plus de 25 ans

d'expérience dans le secteur de la cybersécurité

Plus de 400 millions

de clients utilisent nos produits dans le monde entier

Plus de 200

pays tirent parti de nos solutions

Bibliographie

1. IBM. (2022). Rapport sur le coût d'une violation de données, 2022. IBM.
2. Tilley, A. (2022, 6 octobre). Le manque d'ingénieurs empêche certaines entreprises d'utiliser le cloud. The Wall Street Journal.
3. Deloitte. Six façons de s'attaquer à la pénurie massive de compétences en ingénierie logicielle. Deloitte
4. McKinsey. (2022, 23 juin). Les Américains adoptent le travail flexible – et ils en veulent davantage. McKinsey.
5. Coate, P. (2021, 25 janvier). Le travail à distance avant, pendant et après la pandémie. NCII.
6. Lambert, L. (2020, 22 octobre). 76 % des PDG américains estiment qu'ils pourraient réduire leur espace de bureau. Fortune.
7. PWC. (2022, 17 janvier). 25e enquête mondiale annuelle de PwC auprès des PDG. PWC.
8. IBM et Morning Consult. (2020, 22 juin). Étude sur le travail à domicile. IBM.
9. Verizon. (2022). Rapport d'enquêtes sur les violations de données de 2022. Verizon.
10. Pankov, N. (2020, 15 avril). La menace du Shadow IT. Kaspersky Lab.
11. Kaspersky. (2021, octobre). Le bien-être des employés 2021 : apprendre de la nouvelle réalité. Kaspersky Lab.
12. Posey, C & Shoss, M. (2022, 20 janvier). Recherche : Pourquoi les employés violent les stratégies de cybersécurité. Harvard Business Review.
13. Vergelis, M. (2020, 7 février). Phishing lié au coronavirus. Kaspersky Lab.
14. Proofpoint. (2022). L'état du phishing. Proofpoint.
15. Kaspersky. (2022, 19 juillet). AV-TEST constate que les solutions de sécurité Kaspersky pour les entreprises offrent une protection à 100 % contre les ransomwares. Kaspersky Lab.

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.fr
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com
Catalogue produits pour les entreprises : https://media.kaspersky.com/fr/business-security/enterprise/KL-Enterprise-Catalogue.pdf

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr, dans lequel la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/about/transparency

Proven.
Transparent.
Independent.