kaspersky bring on the future

Le travail à distance sans risque est-il un rêve pour les responsables de la sécurité ou peut-il devenir une réalité ?

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 de ses salariés. Le réseau domestique est le réseau utilisé pour travailler, mais de nombreuses entreprises dépendent de produits de sécurité qui ne peuvent pas les protéger contre la naïveté des employés, et la faible visibilité sur les données est monnaie courante.

Le coût de la négligence est élevé. Les violations de données dans lesquelles le travail à distance intervient coûtent environ un million de dollars de plus que les violations dans lesquelles il ne joue aucun rôle. Examinons les risques auxquels votre entreprise est confrontée.

Risques liés au travail à distance

IBM et Morning Consult ont constaté que les employés qui travaillent à distance pour la première fois représentent un risque plus élevé pour la sécurité, car ils sont généralement trop confiants et mal préparés. Cela accroît la vulnérabilité de votre organisation aux attaques et aux violations de données, mais ces événements **ne sont pas** inévitables. Le risque peut être atténué si vous abordez les points suivants :

- **Dissolution des périmètres** – les politiques BYOD (utilisation d'appareils personnels pour travailler) et le stockage cloud tiers introduisent des risques que les frontières physiques annulaient autrefois
- **Une mauvaise hygiène de sécurité** – un manque de connaissances appropriées peut conduire à une erreur humaine, qui est à l'origine de 82 % des violations de données
- **Shadow IT** – les employés peuvent utiliser des services et des programmes potentiellement dangereux à l'insu de votre service informatique
- **Stresse** – 54 % des employés reçoivent plus de travail, ce qui peut influencer leur comportement (les salariés stressés sont plus susceptibles de commettre des erreurs)
- **Gestion des vulnérabilités** – les outils de collaboration en ligne sont de plus en plus populaires mais peuvent être vulnérables (pensez à Zoom) ; les services informatiques doivent être en mesure de gérer ce risque
- **VPN** – de nombreuses entreprises ont mis en place des outils comme les réseaux privés virtuels (VPN) pour permettre aux travailleurs à distance de travailler, mais même ces outils peuvent être vulnérables

Il peut sembler difficile de faire face à de tels risques, surtout si l'on est une petite ou moyenne entreprise (PME) et que l'on dispose d'un budget limité. Il se peut également que vous n'ayez pas de fonction dédiée à la cybersécurité et que vous ne sachiez pas par où commencer. C'est pourquoi nous avons conçu notre solution de sécurité pour PME, **Kaspersky Endpoint Security Cloud**, pour qu'elle soit complète, abordable et facile à utiliser.

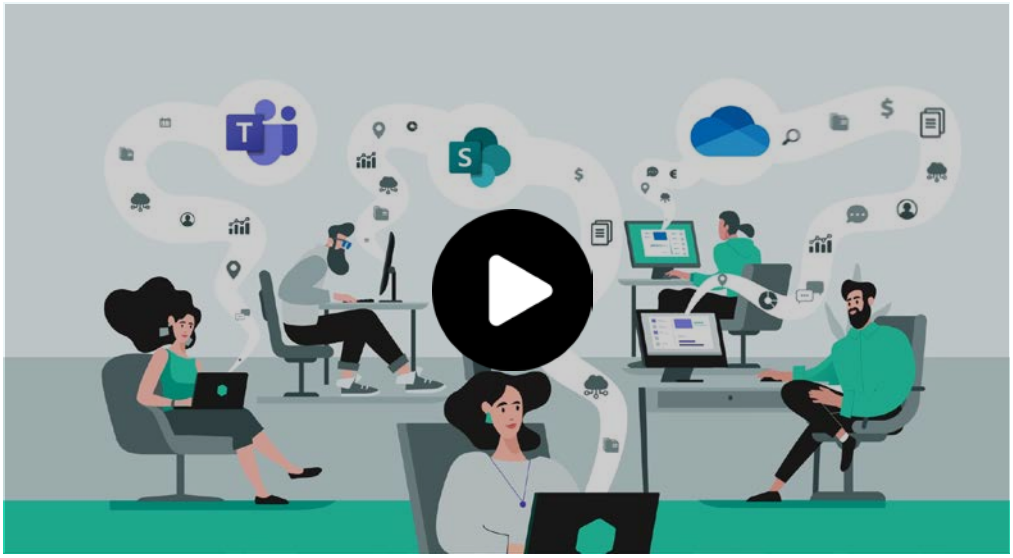
Téléchargez notre **guide étape par étape pour atténuer les cyberrisques dans l'entreprise**

Comment accroître la visibilité

Si vos employés utilisent des services cloud non professionnels, il y a un risque de fuite de données, et il est donc crucial que vos spécialistes informatiques aient une visibilité totale des ressources utilisées. Kaspersky Endpoint Security Cloud vous permet de voir quelles ressources vos employés utilisent, ce qui vous aide à réduire le nombre de services informatiques cloud non contrôlés sur le réseau de l'entreprise, par exemple :

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

En outre, Data Discovery permet une collaboration sécurisée avec Microsoft 365 et vous permet de voir quelles données confidentielles, comme les numéros de passeport et les identifiants de paiement, sont stockées publiquement dans OneDrive. Voici son fonctionnement.



Comment gagner en tranquillité d'esprit

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. C'est pourquoi il est important de mettre en place les bonnes restrictions en ce qui concerne le matériel externe. Kaspersky Endpoint Security Cloud peut limiter l'impact de telles erreurs en interdisant l'utilisation d'appareils externes et en exécutant des analyses automatisées.

Comment en avoir pour son argent

Si vous dirigez une petite entreprise, vous comprendrez l'importance de rentabiliser chaque centime. Et lorsqu'il s'agit de sécurité, le fait de payer le moins de frais possible peut s'avérer très précieux. 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. En fait, notre offre premium est environ **30 % moins chère que la solution équivalente de Microsoft**, couvre 1 000 terminaux et comprend même une formation particulière pour les spécialistes informatiques.

Comment résister à toute épreuve

Kaspersky Endpoint Security Cloud dispose de tout ce dont vous avez besoin pour mener vos activités en toute sécurité. Vous pouvez protéger vos travailleurs à distance où qu'ils se trouvent grâce à notre console basée dans le cloud, quel que soit l'appareil qu'ils utilisent, tandis que le chiffrement à distance garantit la sécurité de vos données en cas de perte ou de vol d'un appareil.

Il est également facile de reprendre le contrôle du cloud, car vous pouvez limiter les services cloud non approuvés ou limiter les accès de certains utilisateurs sur votre réseau afin d'éviter les violations de données. Vous pouvez également activer une coopération et une communication sécurisées dans Microsoft Office 365 grâce à la protection incluse de ses principales applications.

Apprenez-en plus ou commencez votre essai gratuit de 30 jours dès aujourd'hui : Kaspersky Business Hub

Kaspersky
Business Hub

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
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 où 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.