PME : managez facilement votre sécurité à partir du cloud

kaspersky

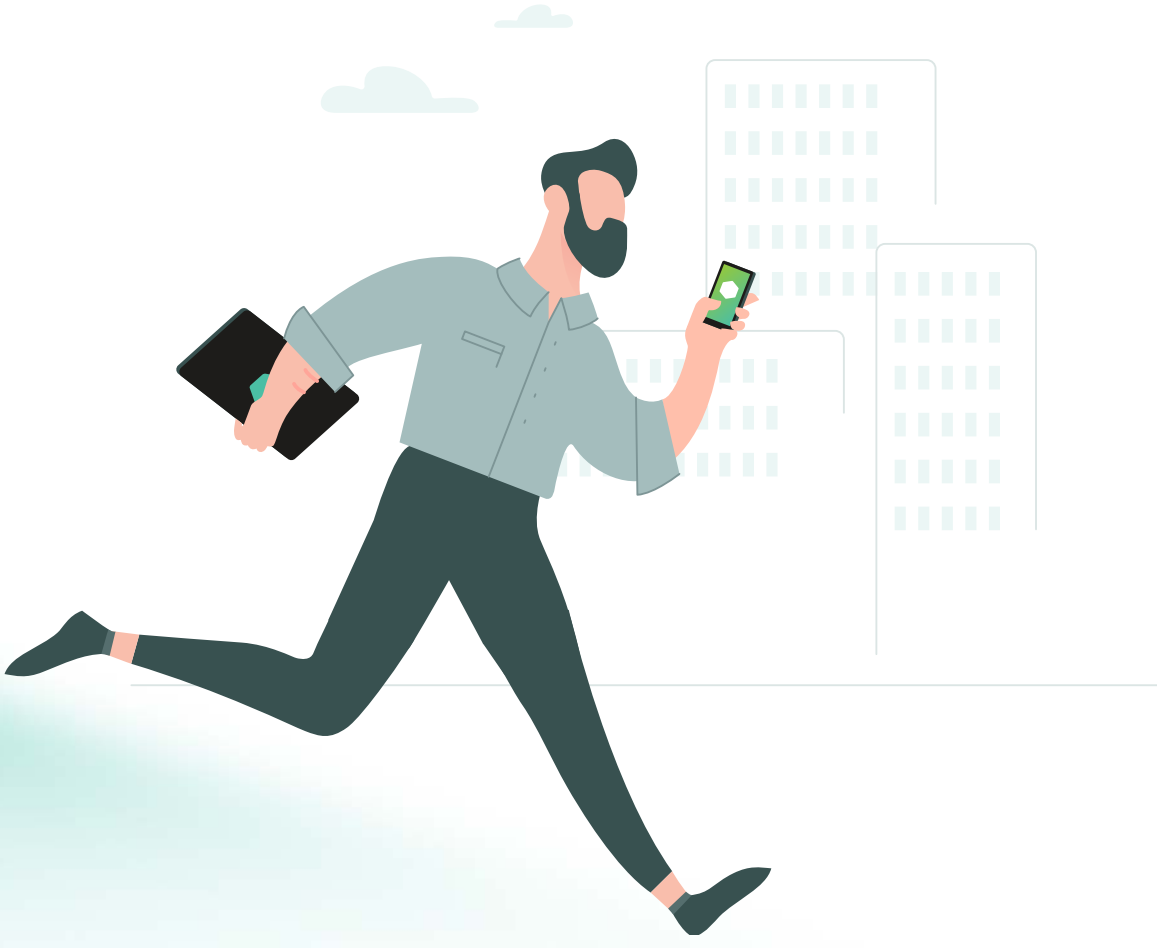
Agilité au quotidien

La solution Kaspersky Endpoint Security Cloud a été conçue pour vous apporter l'agilité dont votre entreprise a besoin

Votre entreprise se développe. Le nombre de tâches de sécurité informatique dont vous devez vous occuper continue de croître lui aussi. Toutefois, vous n'êtes pas encore prêt à recruter un spécialiste dédié à la sécurité. Nous avons donc créé **Kaspersky Endpoint Security Cloud Plus** pour vous aider à gérer facilement les tâches de sécurité de routine, vous faisant ainsi gagner du temps et de l'argent.

Et **Kaspersky Endpoint Security Cloud Pro** ne se limite pas à cela. Cette solution offre la tranquillité d'esprit que procure une protection contre les menaces, même évasives, à mesure que votre sécurité évolue.

La solution Kaspersky Endpoint Security Cloud a été conçue pour vous apporter l'agilité dont votre entreprise a besoin Facile à gérer (interface utilisateur simple, déploiement et opérations faciles, depuis l'intégration des nouveaux salariés jusqu'à la maintenance quotidienne), cette solution permet également de protéger votre entreprise contre les nouvelles cybermenaces.



Enfilez une nouvelle casquette de spécialiste de la cybersécurité grâce à nos fonctionnalités EDR

Commencez par l'analyse des causes profondes (incluse dans notre licence Plus), puis poursuivez avec Kaspersky Endpoint Security Cloud Pro, en ajoutant des options de réponse automatisée, comme l'analyse des indicateurs de compromission (IOC) et l'isolation de l'hôte.

Soyons honnêtes : les administrateurs IT ont de multiples responsabilités, et la cybersécurité n'est pas leur seule priorité. Même si les administrateurs avisés comprennent la nécessité de solutions de cybersécurité efficaces, cela ne relève pas toujours de leurs compétences. Entre-temps, les menaces ne cessent d'évoluer, et celles qui étaient considérées comme rares ou ne visant que les « gros poissons » deviennent courantes et omniprésentes. Il est donc important, d'un point de vue budgétaire, de choisir une solution régulièrement mise à niveau avec des technologies de pointe afin de vous assurer une protection complète pour l'avenir, sans avoir à réaliser d'autres investissements importants.

La solution Endpoint Detection and Response vous donne accès à un outil professionnel de cybersécurité qui optimise la réponse aux menaces évasives et en renforce la détection. Dans le même temps, notre approche garantit une expérience utilisateur EDR globale à la fois simple et harmonieuse, ne nécessitant aucune modification de votre infrastructure.

Notre **analyse des causes profondes** offre des fonctionnalités avancées de détection et de visibilité des menaces, ainsi qu'un accès à des outils professionnels d'enquête sur les incidents, sans qu'il soit nécessaire de modifier votre infrastructure.

En tant qu'administrateur informatique, vous pouvez mener des enquêtes sur les incidents en utilisant le contexte et les détails de l'incident. Vous pouvez effectuer une analyse des causes profondes grâce à la visualisation du chemin de propagation des attaques et en examiner les détails en profondeur :

- Données des hôtes : version du système d'exploitation, interfaces réseau et utilisateurs
- Données des fichiers : nom, hachage, paramètres de création, de modification, de téléchargement, etc.
- Données de traitement : date et heure, paramètres de démarrage
- Détections et incidents associés, etc.

Les options de réponse automatisée vous aideront à bloquer les menaces, en empêchant l'exécution de fichiers grâce à l'isolation de l'hôte et aux vérifications d'analyse IOC (indicateur de compromission). En cas d'attaque, le système isole l'hôte de votre réseau, empêchant ainsi l'attaque de se propager à d'autres appareils. L'analyse IOC vérifie ensuite qu'aucun appareil ne contient d'IOC semblables à ceux impliqués dans l'attaque initiale, et met en quarantaine les appareils qui peuvent être concernés.

Avec une solution de sécurité discrète, vous pouvez protéger le réseau, répondre aux questions et déclencher automatiquement la sonnette d'alarme. Quoi de mieux pour dormir sur vos deux oreilles ?

Mettez un terme au Shadow IT et prenez le contrôle de vos services cloud

Cloud Discovery vous permet de bloquer l'accès non autorisé, inapproprié ou non nécessaire aux ressources dans le cloud, vous permettant de contrôler en toute sécurité vos données tout en garantissant la concentration et la productivité de vos collaborateurs.

Regardez vos collègues : pouvez-vous dire qui perd du temps sur Facebook et qui discute sur messagerie instantanée ? Plus important encore, qui partage des données d'entreprise sur des services de stockage dans le cloud qui vous sont inconnus ? Exactement, vous n'en avez aucune idée. La fonctionnalité Cloud Discovery, incluse dans Kaspersky Endpoint Security Cloud, est là pour vous aider.

Cloud Discovery vous permet d'avoir une vue d'ensemble et d'élaborer un plan d'action. Vous pouvez bloquer l'accès non autorisé, inapproprié ou non nécessaire aux ressources dans le cloud, vous permettant de contrôler en toute sécurité vos données tout en garantissant la concentration et la productivité de vos collaborateurs. Il ne vous suffit que de quelques clics pour en savoir plus sur l'utilisation du cloud au sein de votre infrastructure et ce, via un widget interactif ou un rapport exportable. Muni de ces statistiques, vous pouvez mieux gérer le problème de partage et de divulgation non contrôlé de données d'entreprise, mais aussi le temps passé par les employés sur les réseaux sociaux et les messageries instantanées.

Dans de nombreux cas, cela ouvre des possibilités de croissance. En général, les utilisateurs n'ont pas l'intention de nuire lorsqu'ils utilisent des services cloud non approuvés. Très souvent, ils essaient simplement de travailler de façon plus efficace. Si, par exemple, vous avez mis en place une solution de vidéoconférence d'entreprise ou un CRM dans le cloud, mais que vos utilisateurs continuent d'utiliser des sites publics ou de remplir des tableaux Google Docs, il convient de se demander pourquoi.

Les réponses peuvent vous surprendre. Il peut s'agir de problèmes d'utilisation des logiciels de l'entreprise, de vieilles habitudes d'utilisation, d'un manque de connaissances ou simplement du fait d'avoir manqué un email annonçant les nouvelles stratégies de l'entreprise. De tels problèmes peuvent ralentir la transformation numérique et la croissance globale de l'entreprise. Les analyses de Cloud Discovery peuvent vous aider à mieux former les utilisateurs, mais également à améliorer l'hygiène en matière de sécurité.

Cloud Discovery est une alternative simple et rentable à l'achat d'une solution **CASB (Cloud Access Security Broker)** coûteuse et compliquée. Elle vous aidera à détecter ainsi qu'à bloquer l'utilisation de services cloud non autorisés et le Shadow IT dans le cadre de vos cyberdéfenses standards, et ce, sans que vous ayez besoin de compétences particulières.

Office 365

ALL INCLUSIVE

Solution Security for Microsoft Office 365 incluse

Même avec la fonctionnalité Cloud Discovery intégrée, il se peut que la sécurité de Microsoft Office 365 vous inquiète, à l'instar de nombreuses entreprises. Pour vous aider à prendre le contrôle de votre cloud, nous incluons la protection d'Office 365 avec **Kaspersky Endpoint Security Cloud Plus** et **Pro**. Avec chaque 10 licences, nous fournissons la protection Kaspersky Security for Microsoft Office 365 pour 15 boîtes aux lettres/utilisateurs. **Notre solution de sécurité Microsoft Office 365 propose une protection avancée** tout-en-un contre les menaces pour les services de communication et de collaboration Microsoft Office 365, notamment les suivants :

- **Microsoft Exchange Online, OneDrive, SharePoint Online et Teams**
- **Protection avancée contre les menaces : anti-phishing, protection contre les programmes malveillants et le spam, suppression des pièces jointes indésirables, protection à la demande**

Conformité avec le RGPD en toute simplicité

La conformité avec le RGPD n'est pas négociable, quelle que soit l'ampleur de votre opération. La fonction Data Discovery, également incluse dans **Kaspersky Endpoint Security Cloud Plus** et **Pro**, vous offre la visibilité et le contrôle dont vous avez besoin pour éviter les fuites de données et garantir votre conformité. Désormais, vous pouvez voir exactement où et pourquoi chaque élément de données dont vous êtes responsable est stocké et traité dans le cloud, qu'il s'agisse d'un cloud de données personnelles accessible par des tiers, de données ponctuelles stockées plus longtemps que nécessaire, et bien plus encore. Atteindre une conformité totale devient alors ultra-simple.

Gestion des correctifs pour une sérénité optimale

Personne n'aime appliquer manuellement des correctifs sur les appareils, mais il s'agit d'une tâche qui doit être effectuée régulièrement pour des raisons de cyberhygiène. À l'instar du brossage de dents, c'est ennuyeux mais efficace. Pourquoi ne pas vous épargner cela et déléguer cette tâche à la fonctionnalité de gestion automatique et planifiée des correctifs ? Elle est incluse dans **Kaspersky Endpoint Security Cloud Plus** et **Kaspersky Endpoint Security Cloud Pro**

Chiffrement sans effort des appareils

Il est également possible de gérer le chiffrement de disque FileVault (macOS) et BitLocker (Windows) via la console Kaspersky Endpoint Security Cloud, et d'appliquer le chiffrement à distance, si besoin.

Presque toutes les entreprises collectent différents types d'informations d'identification personnelle, de données financières, de documents confidentiels et autres données sensibles, et les stockent dans leurs systèmes informatiques. Toute divulgation ou perte de données peut non seulement entraîner des amendes et des poursuites, mais aussi avoir des conséquences très néfastes sur toute l'entreprise. Le chiffrement des données permet d'assurer que ces données ne seront pas compromises en cas de violation de votre système ou de perte d'un appareil.

Déploiement efficace d'un agent de terminal : avec ou sans AD (Active Directory) ?

Téléchargez votre client Kaspersky Endpoint Security, puis ajoutez le script de connexion simple fourni dans votre politique de domaine AD

S'il faut installer la protection des terminaux sur quelques ordinateurs seulement, une clé USB suffit. Entre 50 et 100 appareils, le déploiement est plus exigeant mais il reste tout de même rapide et simple.

Kaspersky Endpoint Security Cloud propose deux modes d'installation, choisissez celui qui vous convient le mieux :

1. Déploiement à distance par email

Un lien est envoyé par email sur chaque appareil via la **console Kaspersky Endpoint Security Cloud**. L'utilisateur clique sur le lien pour activer le téléchargement et l'installation de l'application sur le terminal. Le terminal apparaît ensuite dans la liste des appareils protégés sur votre console.

2. Déploiement automatique avec AD (Active Directory)

Téléchargez votre **client Kaspersky Endpoint Security**, puis ajoutez le script de connexion simple fourni dans votre politique de domaine AD. L'application se déploie automatiquement sur vos terminaux et ces derniers apparaissent en tant qu'appareils protégés dans la **console Kaspersky Endpoint Security Cloud**. Consultez les instructions ici.

Lancez-vous et voyez par vous-même !

Pour en savoir plus sur la façon dont Kaspersky Endpoint Security Cloud peut vous aider à protéger facilement votre entreprise, et pour obtenir une version d'essai gratuite, rendez-vous sur le site **https://cloud.kaspersky.com/.**

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

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.