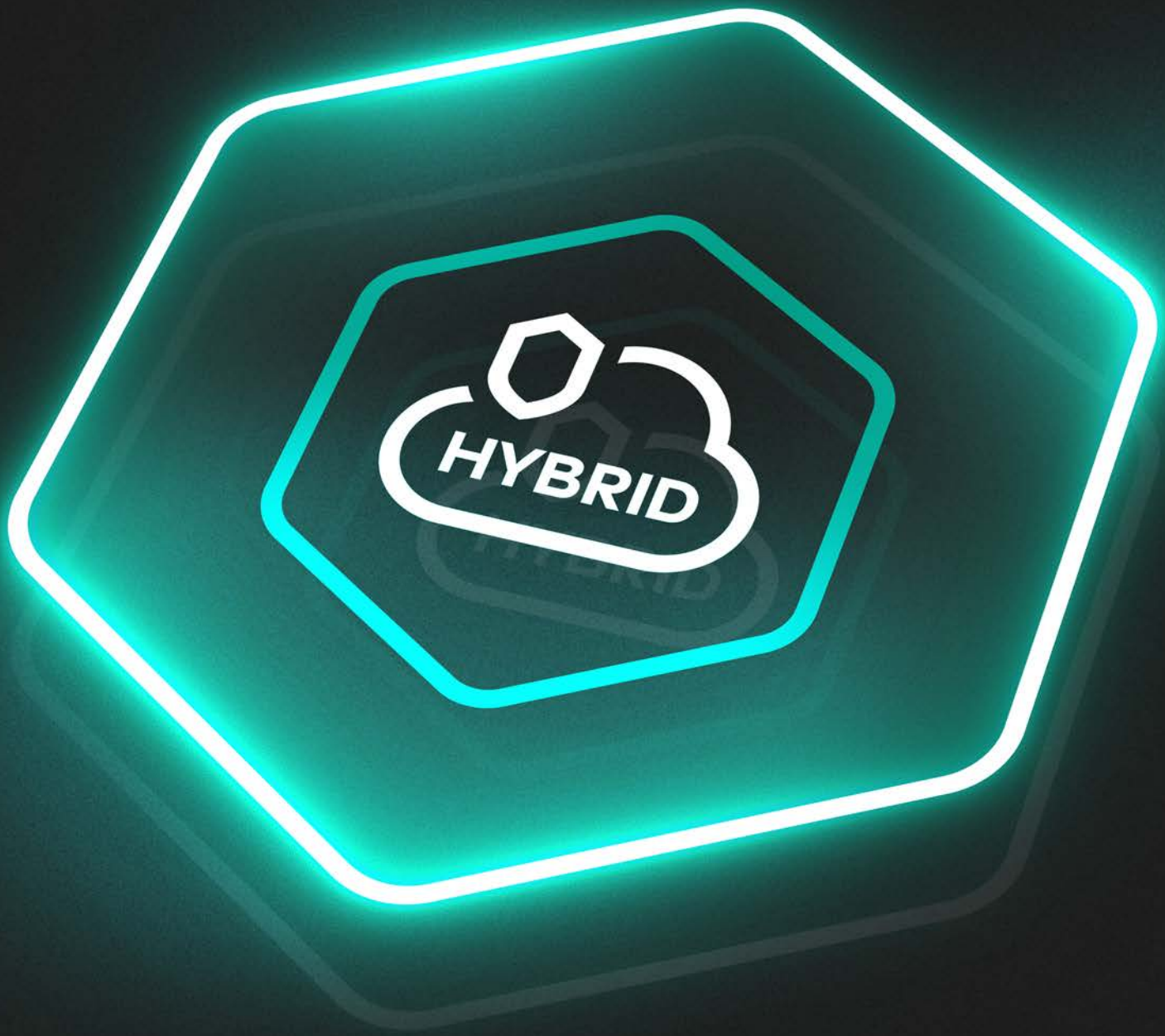


Kaspersky Hybrid Cloud Security

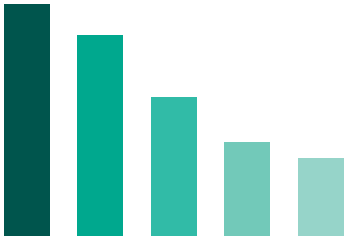
kaspersky PRÊTS POUR L'AVENIR

L'accent mis aujourd'hui par les entreprises sur la transformation numérique entraîne une adoption rapide du Cloud. D'une part, ces initiatives présentent de nombreux avantages pour les entreprises, notamment une plus grande efficacité. D'autre part, les infrastructures deviennent plus complexes, ce qui suscite des préoccupations importantes en matière de risques de sécurité, de gouvernance, de ressources humaines, d'optimisation des performances, de nouvelles réglementations et de dépenses. Kaspersky Hybrid Cloud Security répond à tous ces enjeux.

Une protection éprouvée fonctionnant nativement dans le Cloud et des performances optimales pour vos environnements hybrides

Kaspersky Hybrid Cloud Security rend l'adoption du Cloud, la transformation numérique et les activités commerciales en général plus sûres et plus efficaces. Ce produit unique sécurise l'ensemble de votre infrastructure hybride, en atténuant les risques, en réduisant la consommation de ressources de virtualisation et en soutenant la conformité réglementaire. Kaspersky Hybrid Cloud Security offre une visibilité améliorée et une gestion simplifiée, tout en vous faisant gagner, à vous et à votre équipe, un temps précieux et des ressources budgétaires. La sécurité devient un souci de moins, ce qui vous permet de vous concentrer sur d'autres aspects de votre transformation numérique.

Les principaux défis du Cloud



- Sécurité **81 %**
- Gestion des dépenses relatives au Cloud **79 %**
- Gouvernance et conformité **75 %**
- Gestion du multi-cloud **72 %**
- Migration vers le Cloud **71 %**

Conformément au rapport de Flexera sur l'état du Cloud de 2021

Une protection performante conçue pour répondre aux risques de sécurité des environnements hybrides

- Une protection multi-niveaux contre les menaces lutte de manière proactive contre un large éventail de cyberattaques, y compris les programmes malveillants, les tentatives de phishing et de nombreux autres vecteurs.
- Les algorithmes de machine learning renforcés par l'expertise humaine permettent d'atteindre les plus hauts niveaux de détection et de réduire au minimum le nombre de faux positifs.
- La Threat Intelligence en temps réel permet de se défendre contre les derniers exploits.

Une approche native du Cloud pour une sécurité optimale de l'infrastructure hybride

- Le moteur de cybersécurité protège l'ensemble de l'infrastructure hybride, quelle que soit la charge de travail : physique, virtualisée ou basée dans des Clouds privés, publics et hybrides.
- Une approche compatible avec toutes les plateformes, combinée à une intégration native, permet aux Clouds publics d'être entièrement compatibles avec le système DevOps.
- Les agents légers optimisés pour chaque système d'exploitation réduisent efficacement la consommation de ressources de virtualisation jusqu'à 30 %, les libérant ainsi pour d'autres opérations.

Une rentabilité et une facilité de gestion pour une utilisation confortable du Cloud

- Grâce à un modèle de licence flexible, vous choisissez uniquement les fonctionnalités dont vous avez besoin et tirez le meilleur parti de votre investissement en matière de sécurité.
- Une console dans le Cloud unifiée simplifie la gestion de la sécurité de l'ensemble de votre infrastructure et permet d'économiser les précieuses ressources du personnel informatique.
- L'inventaire simple de l'infrastructure du Cloud et le provisionnement automatisé de la sécurité, quel que soit l'endroit où se trouvent les agents, contribuent à une visibilité maximale.

Sécurité conforme pour les industries hautement réglementées

- Adaptatif et polyvalent, ce produit est conçu pour permettre et soutenir en permanence une conformité réglementaire totale, grâce à des technologies allant du renforcement des systèmes et de l'autodéfense des agents à l'évaluation des vulnérabilités et à la gestion automatisée des correctifs.
- Le large éventail de fonctionnalités permet de s'adapter à la conformité et au paysage des risques, ce qui permet à votre sécurité de rester en permanence à la pointe de la législation actuelle.

Fonctionnalités

Protection multi-niveaux contre les menaces

Threat Intelligence mondiale	Collecte des données en temps réel sur l'état du paysage des menaces, même s'il évolue.
Machine Learning	Les algorithmes de machine learning et l'expertise humaine permettent d'exploiter le Big data de notre Threat Intelligence mondiale.
Protection contre les menaces qui pèsent sur le Web et les emails	Protège les ordinateurs de bureau à distance et virtuels, en les protégeant des menaces basées sur le Web et les emails.
Inspection des journaux	Analyse les fichiers journaux pour une protection opérationnelle optimale.
Analyse comportementale	Protège contre les menaces avancées, notamment les programmes malveillants sans corps ou basés sur des scripts, grâce à la surveillance des applications et des processus.
Moteur d'actions correctives	Annule toutes les modifications malveillantes apportées aux charges de travail du cloud, si nécessaire.
Exploit Prevention	Offre une protection efficace contre la pénétration des menaces, en assurant une compatibilité totale avec les applications protégées, avec une incidence minimale sur les performances.
Fonctionnalités de protection contre les ransomwares	Protège les données critiques de l'entreprise contre toute tentative de demande de rançon, notamment en bloquant le chiffrement à distance et en ramenant les fichiers concernés à leur état antérieur au chiffrement.
Protection contre les menaces réseau	Détecte et empêche les intrusions basées sur le réseau dans les actifs basés dans le cloud.
Protection des conteneurs	Empêche les infections d'être transportées dans l'infrastructure informatique hybride via des conteneurs compromis.

Renforcement du système qui améliore la résilience

Contrôle des applications	Vous permet de verrouiller l'ensemble des charges de travail de votre Cloud hybride en mode de blocage par défaut, pour un renforcement optimal du système, ce qui vous permet de limiter l'exécution aux applications légitimes et fiables uniquement.
Contrôle des périphériques	Indique les appareils virtuels pouvant accéder aux charges de travail individuelles.
Contrôle du Web	Réglemente l'utilisation des ressources Web par les ordinateurs de bureau à distance et virtuels pour réduire les risques et augmenter la productivité.
Système de prévention des intrusions hébergé sur l'hôte (HIPS)	Attribue des catégories de confiance aux applications lancées, limitant ainsi leur accès à des ressources critiques et leurs fonctionnalités.
Surveillance de l'intégrité des fichiers	Contribue à assurer l'intégrité des composants système critiques et autres fichiers importants.
Évaluation des vulnérabilités et gestion des correctifs	Centralise et automatise la sécurité essentielle, les configurations système et les tâches de gestion, telles que l'évaluation de la vulnérabilité, la distribution des correctifs et des mises à jour, la gestion des inventaires et le déploiement d'applications.

Visibilité sans limites

Gestion unifiée de la sécurité	La protection des terminaux et des serveurs pour l'ensemble de l'infrastructure peut être administrée depuis une seule console : au bureau, dans votre data center et dans le Cloud.
Cloud API	L'intégration transparente avec les environnements publics permet la détection de l'infrastructure, le déploiement automatisé de l'agent de sécurité, la gestion basée sur des stratégies et la fourniture simplifiée de l'inventaire et de la sécurité.
Options d'administration flexible	Les capacités multi-clients, une gestion des comptes basée sur les autorisations et un contrôle d'accès basé sur les rôles fournissent une certaine flexibilité tout en conservant les avantages de l'orchestration unifiée à partir d'un serveur unique.
Intégration SIEM	Permet l'intégration du produit avec le système de gestion et d'information de la sécurité, réunissant en un seul endroit les différents aspects de la cybersécurité de l'entreprise sur l'ensemble du réseau informatique hybride.

Pourquoi choisir Kaspersky Hybrid Cloud Security ?

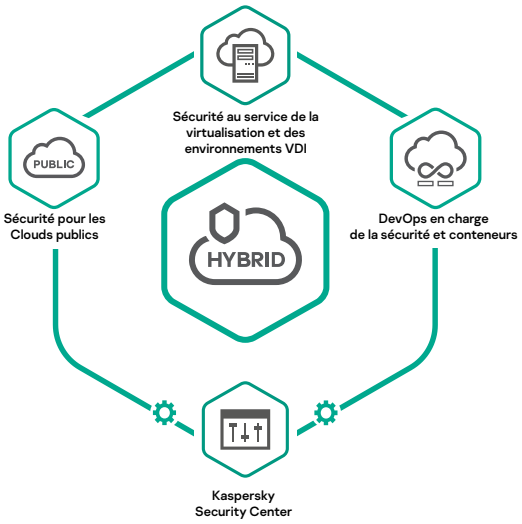
30 %

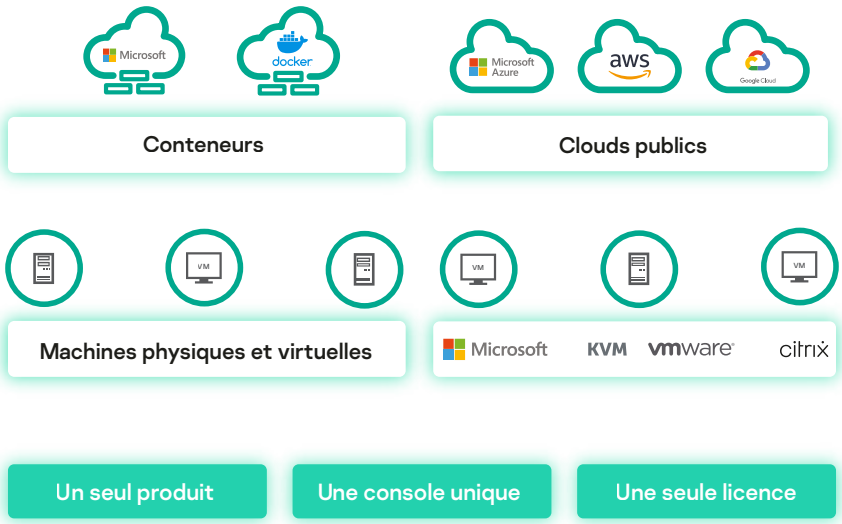
des économies potentielles sur les ressources matérielles de virtualisation par rapport à l'utilisation d'une solution traditionnelle de sécurité des terminaux.

TOP3

des performances exceptionnelles et durables. L'année dernière, les produits Kaspersky ont une fois de plus atteint des niveaux de performance exceptionnels dans de nombreux tests indépendants, obtenant 57 premières places et 63 places parmi les trois meilleures solutions (pour en savoir plus, consultez le site kaspersky.fr/top3).

Un seul produit pour tous vos besoins en matière de sécurité du Cloud





Un seul produit | **Une console unique** | **Une seule licence**

Avis clients

« Cette solution permet de protéger les environnements virtuels et Cloud, sans avoir aucune incidence sur les performances du système ni perturber l'expérience utilisateur. »

« Excellent moyen de combiner toutes les solutions de sécurité en une seule licence. »

« Il n'est pas nécessaire d'installer des logiciels antivirus ni d'autres agents supplémentaires. »

« Une solution centralisée dans le Cloud pour la protection des données. Au même endroit. »

« La protection s'applique instantanément à toutes les VM, car il n'est pas nécessaire de télécharger de nouvelles mises à jour. »

« La solution optimale qui ne requiert pas de longue formation des administrateurs. »

Tiré des avis d'Amazon et de Gartner

Demander une démonstration

www.kaspersky.fr