Kaspersky® Hybrid Cloud Security

Une protection éprouvée pour votre Cloud hybride

Principaux défis des utilisateurs du Cloud :

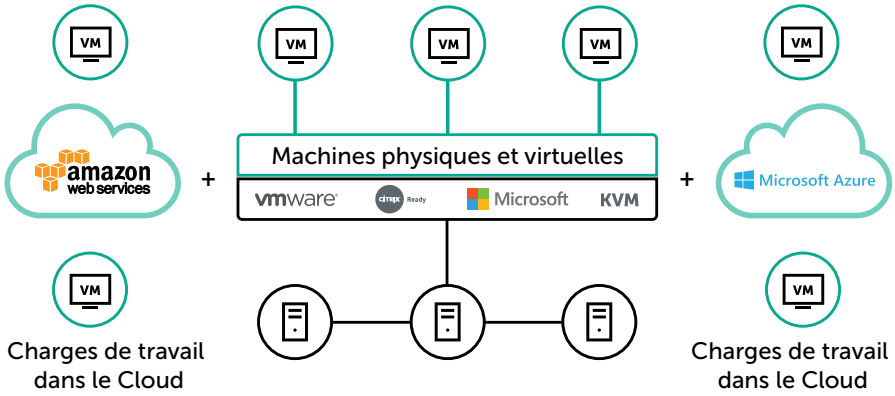
- La complexité grandissante de l'infrastructure peut se traduire par moins de transparence
- Une approche multi-niveaux, la clé d'une protection fiable, est rarement disponible dans un seul produit
- Les solutions de sécurité traditionnelles réduisent les ressources système précieuses
- L'approche en silo et les différents contrôles entraînent des défis administratifs et de sécurité supplémentaires
- Les programmes malveillants et les ransomwares ciblent les terminaux virtuels et physiques
- L'échec de l'application de mesures de cybersécurité adaptées pour la protection de données personnelles peut entraîner des problèmes juridiques.

Pourquoi choisir Kaspersky Hybrid Cloud Security ?

- Conçu pour les charges de travail physiques, virtuelles et dans le Cloud
- Sécurité multi-niveaux intégrée pour tous les types de charges de travail
- Sécurité cohérente, automatisée et flexible pour les Clouds publics AWS et Azure
- Contribue à respecter les responsabilités partagées grâce à un ensemble complet d'outils de sécurité
- Gestion de la sécurité simplifiée dans l'ensemble de votre Cloud hybride
- La protection la plus testée et la plus sécurisée, selon de nombreuses récompenses et tests indépendants[1]
- Basée sur des technologies qui ont gagné la reconnaissance et la confiance des clients, et notamment le prix Platinum Customer Award de Gartner Peer Insights.

La virtualisation est devenue une démarche pilier pour chaque entreprise qui essaie d'être flexible et efficace. Le Cloud computing s'impose naturellement comme l'étape suivante. Il atténue les contraintes de la prise en charge des infrastructures complexes et offre un niveau d'efficacité inaccessible auparavant. Toutefois, le parcours dans le Cloud comporte des complications et des risques, nouveaux pour certains et issus du monde physique pour d'autres.

Kaspersky Hybrid Cloud Security vous offre une sécurité unifiée pour toutes les étapes ou les scénarios de votre parcours dans le Cloud. Adaptée pour la migration dans le Cloud et les scénarios de Cloud natif, cette solution sécurise vos charges de travail physiques et virtuelles, qu'elles fonctionnent sur site, dans un data center ou dans un Cloud public. Ses applications ayant été créées pour s'adapter au fonctionnement du serveur et à la virtualisation, elle offre une protection équilibrée contre les menaces actuelles et futures les plus avancées, sans compromettre les performances du système.



Principaux avantages

Cette solution permet une expérience sécurisée dans le Cloud, sans compromettre les niveaux de protection

- Les technologies brevetées et notre moteur de cybersécurité primé sécurisent toutes vos charges de travail, physiques, virtuelles ou basées sur le Cloud.
- La protection multi-niveaux en temps réel, reposant sur le Machine Learning, sécurise vos données, vos processus et applications contre les menaces émergentes.
- L'approche holistique de la sécurité des données contribue à réduire les risques juridiques et de réputation relatifs aux réglementations sur la protection des données.

1 Les tests couvrent une gamme de produits Kaspersky Lab basés sur les mêmes technologies de protection contre les menaces utilisées dans Kaspersky Hybrid Cloud Security.

Approche Kaspersky HuMachine™

Basé sur la fusion en toute transparence de la Threat Intelligence à partir du big data, des capacités de machine learning robotiques et de l'expérience d'experts humains, Kaspersky HuMachine™ offre plusieurs avantages et assure une protection plus efficace. En combinant chaque élément, les composants individuels gagnent en puissance pour proposer une solution encore plus efficace.

La solution vous permet d'exploiter au mieux vos ressources et vos investissements

- La protection basée sur un agent léger ou sans agent sécurise les actifs virtualisés sur les réseaux standard et à définition logicielle (SDN), sans nuire aux performances.
- L'intégration avec la sécurité native du Cloud géré et public permet de sécuriser vos applications, vos systèmes d'exploitation, vos flux de données et les espaces de travail de vos utilisateurs avec le plus faible encombrement de ressources possible.
- La gestion unifiée des ressources physiques et virtuelles permet d'économiser des heures de travail lors de l'adoption et de la maintenance.

La solution offre une visibilité et un contrôle transparents, indépendamment de la configuration de votre infrastructure hybride

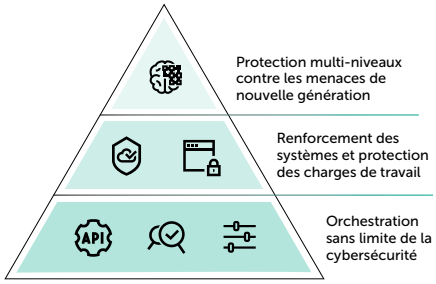
- L'administration de la sécurité fonctionne parfaitement à travers les multiples Clouds.
- La solution assure la visibilité complète, le contrôle et la protection holistique contre les menaces les plus avancées pour chaque charge de travail, dans tous les Clouds.
- Les services de sécurité et les opérations basées sur des stratégies sont fournis plus facilement dans tout votre Cloud hybride.

Fonctionnalités

Protection multi-niveaux des menaces grâce à la surveillance HuMachine

La protection contre les programmes malveillants de nouvelle génération de Kaspersky Lab comprend plusieurs niveaux de sécurité proactifs capables de bloquer une large gamme de cyberattaques menaçant vos charges de travail stratégiques.

- La **Threat Intelligence mondiale** fournit des données en temps réel sur l'état de l'environnement des menaces, même en cas de mutation, pour assurer votre protection à tout moment.
- **Machine Learning :** Le « big data » issu de la Threat Intelligence mondiale est traité grâce à la puissance des algorithmes de machine learning combinée à l'expertise humaine, assurant par là même des niveaux de détection élevés en minorant les faux positifs.
- La **protection contre les menaces Web et de messagerie** permet d'assurer un fonctionnement sécurisé des ordinateurs de bureau à distance et virtuels, en les protégeant des menaces basées sur le Web et les emails.
- La **surveillance de l'intégrité des fichiers** permet d'assurer l'intégrité des composants système critiques et autres fichiers importants.
- L'**inspection des journaux** analyse les fichiers journaux internes pour une protection opérationnelle optimale.
- L'**analyse comportementale** surveille les applications et les processus et les protège contre les menaces les plus sophistiquées, y compris les programmes malveillants sans corps ou basés sur un script.
- Le **moteur d'actions correctives** annule toutes les modifications malveillantes apportées aux charges de travail du Cloud, si nécessaire.
- La **prévention des vulnérabilités** offre une protection efficace contre la propagation des attaques, tout en garantissant une parfaite compatibilité avec les applications protégées et un impact minimal sur les performances.
- La **fonctionnalité de protection contre les ransomwares** protège les charges de travail virtuelles contre toute tentative de violation des données stratégiques de l'entreprise, en rétablissant les fichiers affectés à leur état préchiffré et en bloquant à distance le chiffrement lancé.
- La **protection contre les menaces réseau** détecte et empêche les intrusions basées sur le réseau dans les actifs basés dans le cloud.



Sécurité unifiée pour tous les Clouds

Les clouds publics
- Amazon Web Services (AWS)
- Microsoft Azure

Data centers privés
- Vmware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Proxmox

Environnements VDI
- Vmware Horizon
- Citrix XenDesktop

Serveurs physiques
- Windows
- Linux

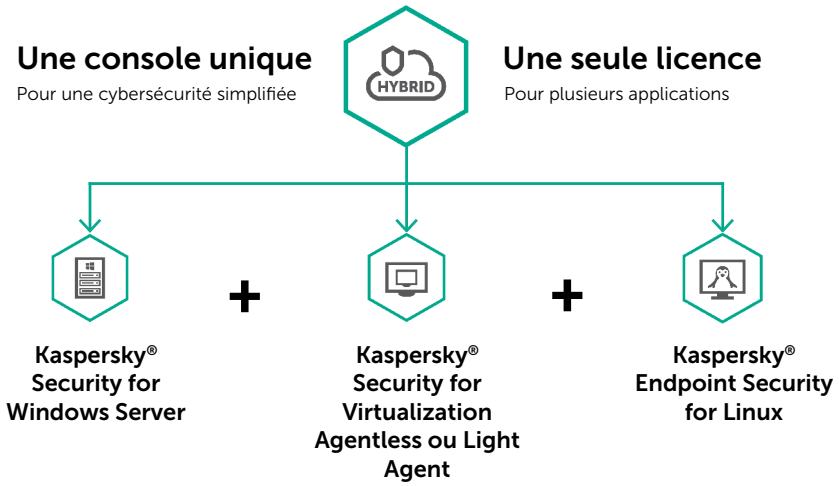
Le renforcement du système améliore la résilience

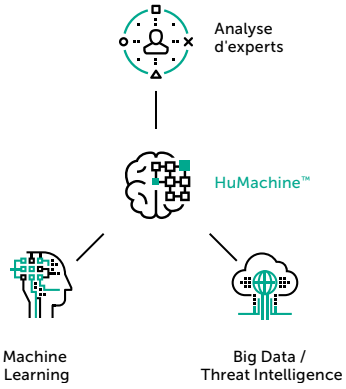
- Les **contrôles des applications** vous permettent de verrouiller l'ensemble des charges de travail de votre Cloud hybride en mode de blocage par défaut, pour un renforcement optimal du système, ce qui vous permet de limiter l'exécution aux applications légitimes et fiables uniquement.
- Les **contrôles des appareils** indiquent les appareils virtuels pouvant accéder aux charges de travail individuelles.
- Le **contrôle Web** réglemente l'utilisation des ressources Web par les ordinateurs de bureau à distance et virtuels pour réduire les risques et augmenter la productivité.
- Le **Système de prévention des intrusions hébergé sur l'hôte avec pare-feu individuel (HIPS)** attribue des catégories de confiance aux applications lancées, limitant ainsi leur accès à des ressources critiques et leurs fonctionnalités.

Visibilité sans limite

- La **gestion de sécurité unifiée** du Kaspersky Security Center facilite l'administration centralisée de la sécurité à travers l'ensemble de l'infrastructure, des terminaux et des serveurs, au bureau, dans votre data center et dans le Cloud.
- **API du Cloud :** L'intégration transparente avec les environnements AWS et Azure 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.
- Les **options de gestion flexibles** fournissent des capacités multi-clients, une gestion des comptes basée sur les autorisations et un contrôle d'accès basé sur les rôles, ce qui permet une certaine flexibilité tout en conservant les avantages de l'orchestration unifiée à partir d'un serveur unique.
- **Intégration SIEM :** Dans les infrastructures dotées de systèmes informatiques plus matures, des systèmes de gestion et d'information sur la sécurité peuvent être utilisés comme un aperçu unifié des différents aspects de la cybersécurité de l'entreprise, à travers l'ensemble du réseau informatique hybride.

Kaspersky Hybrid Cloud Security offre des technologies de sécurité plusieurs fois primées et reconnues par l'industrie pour prendre en charge et simplifier la transformation de votre environnement informatique. Cette solution sécurise la migration d'un environnement physique à un environnement virtuel et dans le Cloud et garantit la visibilité et la transparence nécessaires pour une orchestration de sécurité optimale.





Kaspersly Lab
Solutions de sécurité pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **www.securelist.com**
Notre approche unique : **https://www.kaspersky.fr/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.fr