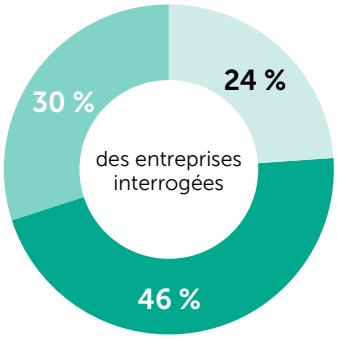
Kaspersky® Hybrid Cloud Security

Protège votre Cloud Amazon Web Services

Les Clouds publics et gérés font maintenant partie de l'environnement informatique de l'entreprise. On reconnaît de plus en plus que les Clouds publics comme Amazon Web Services (AWS) ont suffisamment évolué pour être capables de supporter des charges de travail critiques.

Ces fonctionnalités ont un impact sur la vision de la sécurité des entreprises et sur la construction de leurs stratégies informatiques. Comment l'infrastructure informatique va-t-elle s'adapter et évoluer au cours des trois à cinq prochaines années ? Comment exploiter au mieux les fonctionnalités des Clouds publics et gérés, tout en assurant la sécurité et l'efficacité de l'infrastructure hybride correspondante ?

Les incidents de cybersécurité représentent toujours une grande source de préoccupation pour les entreprises et un nombre croissant d'entre elles en subissent les conséquences financières, de réputation et parfois juridiques. La sécurité de l'entreprise doit être suffisamment agile et intelligente pour lutter contre les menaces actuelles et futures. Elle doit également proposer l'évolutivité et la souplesse nécessaires pour s'adapter et évoluer parallèlement à votre environnement de Cloud hybride, intégrant à la fois les fonctionnalités des Clouds publics et privés.



- utilisent le Cloud, mais n'ont pas encore effectué d'audit ou de vérification de conformité
- utilisent le Cloud, mais n'ont pas mis en place de plan d'atténuation des menaces
- ont adopté les technologies dans le Cloud avec un plan d'atténuation des menaces entièrement testé

Source : Rapport 2017 sur la maintenance du contrôle et de la sécurité des données dans le Cloud de Kaspersky Lab

Clouds privés et publics : votre environnement hybride

La sécurisation de votre Cloud privé est une tâche relativement simple. L'utilisation de la virtualisation pour créer un data center logiciel est une pratique relativement établie. Kaspersky Lab propose un logiciel spécialisé conçu pour offrir le plus léger encombrement possible sur la machine virtuelle (ou, dans le cas de VMware, aucun encombrement du tout) pour optimiser l'efficacité et conserver les économies de ressources et la flexibilité fournies par la technologie de virtualisation.

Cependant, le transfert du Cloud privé vers le Cloud public, en particulier la transition entre les deux, a soulevé de nouveaux problèmes. Où commence et s'arrête votre responsabilité en termes de sécurité ? Comment gérez-vous et protégez-vous les charges de travail lorsqu'elles sont déplacées des Clouds en interne et hors site ?

Les menaces de sécurité et leur atténuation

Les environnements Cloud extensibles sont confrontés à plusieurs risques, indépendamment de leur taille, des plateformes de virtualisation utilisées dans le data center privé software-defined ou de la plateforme de Cloud choisie pour exécuter les applications professionnelles stratégiques. Les fournisseurs de services de Cloud, comme Amazon, font en sorte que les Clouds publics restent un hébergement sécurisé pour les utilisateurs du Cloud de toutes tailles. AWS fournit toute une gamme d'outils de sécurité natifs très efficaces pour la création d'environnements professionnels sans limite. Cependant, il existe toujours un risque.

Chez Kaspersky Lab, nous constatons un certain nombre de menaces graves (pas seulement en termes de cybersécurité) qui peuvent avoir des incidences négatives sur vos stratégies d'adoption du Cloud et ralentir votre transformation numérique.

Fuites ou violations de données

Pour empêcher les violations de données, Kaspersky Lab recommande d'appliquer des cyberdéfenses pour chaque charge de travail individuelle dans votre environnement de Cloud hybride. La visibilité et la transparence des niveaux informatiques et de sécurité sont essentielles pour vous permettre de visualiser chaque charge de travail exigeant une protection et fournir des capacités de cybersécurité automatisées à l'ensemble de votre environnement de Cloud extensible et en constante évolution.

La visibilité de l'infrastructure est un problème dans les environnements numériques extensibles. Votre cybersécurité peut également avoir perdue en transparence, de sorte que vous ne pouvez pas toujours localiser précisément les zones à risques, ni quand elles surviennent. Même si vous les connaissez, il est souvent trop tard. Avec cette sécurité fragmentée, les Clouds hybrides représentent une cible idéale pour les cybercriminels, notamment car les mêmes outils peuvent être utilisés pour pénétrer les infrastructures traditionnelles et de Cloud. Une violation de données peut exposer des informations sensibles sur les clients ou les partenaires, la propriété intellectuelle et les secrets commerciaux, pouvant engendrer de graves conséquences.

Perte de données ou perte d'intégrité

Le moyen le plus efficace pour assurer l'intégrité des données est de mettre en place des outils de cybersécurité offrant des capacités de protection à l'exécution performantes, associés à des analyses comportementales s'appuyant sur le Machine Learning. Ces fonctionnalités permettent l'identification des menaces cachées les plus avancées ou des programmes de ransomware les plus sophistiqués.

Les violations de données sont généralement le résultat d'une activité malveillante. Il existe cependant plusieurs scénarios possibles lorsque vos données sont inaccessibles ou endommagées suite à une série d'actions volontaires ou non de vos utilisateurs finaux ou à une activité malveillante. La plupart des organisations disposent de stratégies de récupération de données permettant d'assurer un RTO (objectif de temps de récupération) le plus bas possible et un RPO (objectif de point de récupération) le plus court possible. Toutefois, malgré la sauvegarde ou la réplication de vos données, vous pourrez rencontrer quelques mauvaises surprises lors des restaurations futures. Le nombre croissant d'attaques de ransomwares réussies et très dommageables contre des entreprises de tout type confirme que le maintien de l'intégrité des données est une mission difficile. Peu importe l'âge des données ou l'emplacement des charges de travail physiques, virtuelles ou dans le Cloud, la perte de données ou d'intégrité représente des risques importants.

Applications vulnérables ou indésirables

Kaspersky Lab sait exactement comment lutter contre ces attaques. Les meilleures stratégies de cyberdéfense sont fondées sur une combinaison de contrôles au démarrage des applications (liste blanche, blocage par défaut) et de fonctions de prévention des vulnérabilités.

Au sein des entreprises, les utilisateurs finaux installent et travaillent sur une large gamme de systèmes et d'applications, et vous ne pouvez pas toujours contrôler les éléments installés sur les appareils des utilisateurs finaux ou même sur les serveurs stratégiques. Plus l'environnement de l'entreprise est vaste, plus il est difficile de tout contrôler. Même les applications stratégiques avec lesquelles vous travaillez régulièrement peuvent ne pas être résistantes aux vulnérabilités « zero-day » et aux exploits, et nécessitent des mesures correctives contre les éventuels risques de cybersécurité.

Sécurité gourmande en ressources

Il est important de comprendre qu'il est de votre responsabilité d'avoir une vision d'ensemble très claire de tous les composants de votre Cloud hybride et de mettre en œuvre des fonctions de cybersécurité qui fourniront la protection la plus efficace et une utilisation des ressources adaptée.

La plupart des Clouds hybrides fonctionnent comme une combinaison de data centers privés software-defined et de services de Cloud public extensibles. Ces deux infrastructures nécessitent une protection adaptée, associant des technologies fournissant des capacités d'intégration différentes. L'adoption d'une approche traditionnelle prônant l'application d'un antivirus partout dans les Clouds hybrides entraîne une utilisation massive et inefficace de vos ressources de Cloud, qui compromet l'efficacité des systèmes stratégiques de l'entreprise et réduit considérablement le retour sur investissement de la transformation numérique.

Alignement de la sécurité et de l'infrastructure inadapté

Kaspersky Hybrid Cloud Security offre une intégration native via une API qui permet une connexion fiable entre les niveaux informatique et de sécurité du Cloud à mettre en place, afin que ces niveaux puissent fonctionner ensemble, en s'appuyant sur leurs capacités respectives. Ces fonctionnalités comprennent la détection d'infrastructure automatisée et la fourniture de mesures de sécurité, quelle que soit la taille de votre environnement Cloud hybride.

L'adoption du Cloud hybride favorise un nouveau dynamisme et un inventaire efficace, mais aussi l'application constante de mesures de cybersécurité sur des centaines de charges de travail nouvellement déployées dans le Cloud. Cette situation peut vite devenir problématique. L'équipe chargée de la sécurité a limité ou retardé la visibilité des machines dans le Cloud, qui se sont multipliées. Ces machines restent donc vulnérables jusqu'à la prochaine analyse du réseau de l'entreprise. Des outils automatisés utilisés par le personnel informatique généraliste pour exécuter des tâches administratives, telles que la segmentation du réseau, l'isolement et la reconfiguration de la topologie peuvent s'avérer très utiles pour répondre rapidement aux nouvelles cybermenaces et contribuer à l'adoption de principes de diligence raisonnables. Si votre informatique et votre sécurité n'interagissent pas, les équipes de sécurité ne pourront pas protéger ce qu'elles ne voient pas et les informaticiens généralistes ne seront pas en mesure de les aider à mettre en place un véritable écosystème sécurisé et évolutif pour l'ensemble du Cloud hybride.

Pourquoi choisir Kaspersky Hybrid Cloud Security ?

1. Conçu pour les charges de travail physiques, virtuelles et dans le Cloud
2. Sécurité multi-niveaux intégrée pour tous les data centers privés
3. Sécurité simple, automatisée et flexible pour les Clouds publics AWS et Azure
4. Contribue à respecter les responsabilités partagées grâce à un ensemble complet d'outils de sécurité
5. Gestion de la sécurité au niveau de l'entreprise dans l'ensemble du Cloud hybride

Responsabilité partagée dans les Clouds publics

Les Clouds publics comprennent un système de sécurité intégré. Le modèle de responsabilité partagée impose que vos charges de travail, vos applications et vos données dans les Clouds publics restent à votre charge. Lorsque ces charges de travail sont stratégiques, cette responsabilité devient encore plus importante.

AWS est le principal fournisseur de Cloud public ; il offre l'environnement le plus perfectionné du marché avec une fiabilité et une évolutivité exceptionnelles et fournit une gamme d'outils de sécurité natifs Cloud.

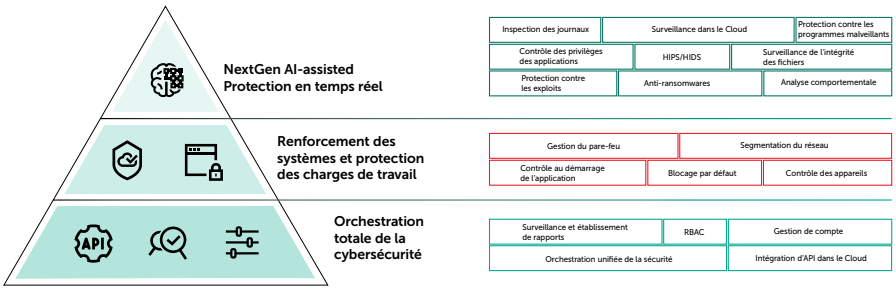
Toutefois, la responsabilité de la sécurité partagée exige des fonctionnalités de sécurité supplémentaires, permettant la mise en place d'un niveau de cybersécurité extensible qui englobe l'ensemble de votre environnement Cloud, public et privé, et qui protège les données que vous possédez sur votre parc AWS.

Sécurité intégrée pour les Cloud AWS

La philosophie de Kaspersky Lab a été de créer une solution parfaitement équilibrée associant une protection haut de gamme, une cybersécurité économe en ressources et des fonctionnalités de mise en œuvre pour votre environnement AWS. Nous le faisons mieux que quiconque, en partie grâce à l'intégration via l'API AWS.

En collaborant avec AWS, nous vous proposons d'abord des capacités de cybersécurité innovantes et de « nouvelle génération », basées sur le moteur de protection le plus récompensé[1] et le plus testé[2] du secteur actuellement. La cybersécurité de nouvelle génération repose sur un fonctionnement humain-machine, afin de concevoir un environnement de sécurité dans le Cloud adaptatif et extensible. Voilà le type de service que nous proposons. Vous serez en capacité de détecter et de réagir aux cybermenaces les plus avancées.

- **Notre moteur de protection contre les programmes malveillants primé** assure une protection au niveau des fichiers, automatique et en temps réel pour toutes les charges de travail dans le Cloud, à l'accès et à la demande.



- **Une surveillance dans le Cloud** identifie rapidement les nouvelles menaces et fournit des mises à jour automatiques
- **La détection comportementale** surveille les applications et les processus, protège contre les menaces les plus sophistiquées et les programmes malveillants sans corps et annule toute modification malveillante effectuée à l'intérieur des charges de travail du Cloud si nécessaire.
- **La protection contre les vulnérabilités** contrôle les applications et les processus d'exploitation des systèmes, contribue à bloquer les menaces avancées, y compris les ransomwares.
- **La protection contre les ransomwares** protège les charges de travail Cloud et leurs réseaux partagés contre les attaques, et rétablit tout fichier affecté à son état préchiffré.
- **Le système HIPS/HIDS** détecte et prévient les intrusions basées sur le réseau dans les actifs basés dans le Cloud.
- **Les contrôles d'applications** permettent de verrouiller toutes les charges de travail dans le Cloud hybride en mode blocage par défaut pour un renforcement des systèmes optimal, et imposent l'emplacement de l'exécution des applications et les éléments auxquels elles peuvent accéder.
- **Le contrôle des appareils** spécifie les appareils virtualisés pouvant accéder aux charges de travail individuelles dans le Cloud, alors que le contrôle Web protège contre les cybermenaces basées sur Internet.
- **La segmentation du réseau** fournit une visibilité et une protection automatisée des réseaux d'infrastructure du Cloud hybride.

Protection, visibilité et facilité de gestion optimales

L'intégration de nos capacités de cybersécurité avancée avec celles d'AWS à travers son API apporte d'autres avantages :

- **Efficacité des systèmes**
  L'inventaire de l'infrastructure du Cloud devient beaucoup plus simple, comme la fourniture de la sécurité automatisée de vos instances AWS EC2, quel que soit leur emplacement. L'efficacité de ces systèmes peut générer d'importantes économies en termes de temps et de ressources.
- **Visibilité totale**
  La visibilité peut devenir problématique dans les environnements de Cloud hybride, et ici encore l'intégration étroite est efficace. L'intégration via l'API AWS vous permet d'avoir une vision à 360°, de comprendre l'organisation de votre Cloud et de vous assurer que l'ensemble des charges de travail de votre Cloud est protégé.
- **Orchestration simplifiée**
  L'intégration de l'API AWS garantit la gestion unifiée de toutes vos ressources informatiques, sur site et dans le Cloud, via une console unique, offrant une visibilité et une transparence complètes et permettant une orchestration et une administration fluides et efficaces.
- **Sécurité « pour » et « par » le Cloud**
  Notre protection pour AWS EC2 est également disponible sur le site de e-commerce AWS, pour fluidifier, simplifier et sécuriser votre migration vers le Cloud. Quoi de mieux que le meilleur système de sécurité pour le Cloud, disponible depuis le Cloud ?
- **Licence flexible**
  Les différentes options de licence et de tarification, notamment les options BYOL (Bring Your Own Device) et PPU (Pay-Per-Use), permettent d'optimiser votre investissement dans la transformation numérique et informatique et d'assurer un retour sur investissement intéressant pour votre projet d'adoption du Cloud.

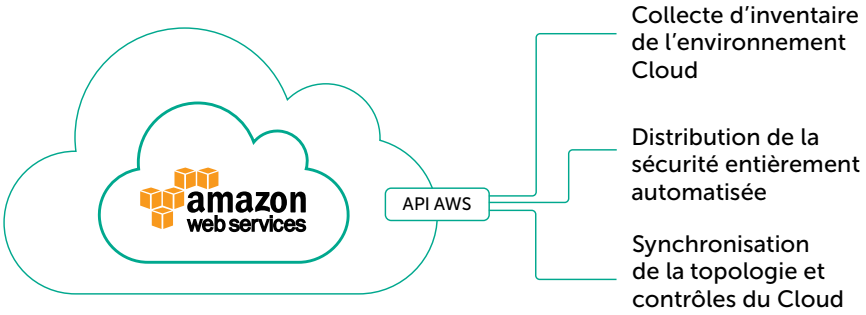
1 https://www.kaspersky.fr/top3
2 https://www.gartner.com/newsroom/id/3807164

- **Les boucliers contre les vulnérabilités** empêchent les programmes malveillants avancés et les menaces « zero-day » d'exploiter des vulnérabilités non corrigées
- **Mail security** comprend une protection contre le spam et protége le trafic de messagerie dans les charges de travail dans le Cloud.
- **Web security** inclut une protection contre le phishing et protège contre les menaces provenant de scripts et de sites Web potentiellement dangereux.
- **La surveillance de l'intégrité des fichiers** protège les fichiers système critiques, alors que l'inspection du journal analyse les fichiers journaux internes pour assurer la sécurité opérationnelle.

Toutes ces fonctionnalités, couvrant votre environnement de serveurs physiques et virtuels et les ressources basées dans le Cloud AWS sont fournies dans un seul produit Kaspersky Lab, géré via une console de sécurité unifiée.

Fonctionnalités de sécurité

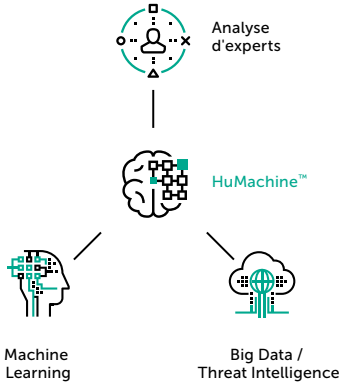
En déployant cette solution de sécurité multi-niveaux à l'ensemble de votre infrastructure de Cloud privé et public, vous avez l'assurance de savoir que toutes vos données, processus et applications sont protégés par une sécurité globale performante.



Sécurisation de la future infrastructure informatique de l'entreprise

Amazon Web Services est en train de changer la structure du service informatique de l'entreprise. Chez Kaspersky Lab, nous garantissons la sécurité, la visibilité et la facilité de gestion de vos charges de travail, à travers votre parc Cloud AWS et votre environnement de Cloud privé, aujourd'hui et à l'avenir.

Kaspersky Hybrid Cloud Security offre de multiples technologies de sécurité reconnues par l'industrie pour prendre en charge et simplifier la transformation de votre environnement informatique, en sécurisant votre migration du physique vers le virtuel et vers le Cloud, tandis que sa visibilité et sa transparence garantissent une expérience d'orchestration de sécurité sans faille.



Kaspersky 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