Solutions de cybersécurité
de Kaspersky Lab pour les entreprises

KASPERSKY lab

Sécurité de votre data center privé : faites le bon choix

www.kaspersky.fr
#truecybersecurity

Sécurité de votre data center privé : le bon choix

Objectif de ce document

Le modèle de conception des data centers d'entreprise a profondément évolué et ces derniers sont de plus en plus définis par logiciel. Les concepts de virtualisation des ressources IT qui font leurs preuves depuis des années sont également applicables dans d'autres secteurs. La virtualisation de l'infrastructure réseau en est un exemple. Les technologies de virtualisation sont depuis longtemps la norme pour les entreprises (d'après les statistiques de 2016, le taux de pénétration des technologies de virtualisation dans les entreprises atteint 75 %). Cette transition a pour but de transférer la gestion des data centers d'entreprise de l'infrastructure aux processus métier.

Naturellement, tous ces changements nécessitent une refonte des politiques de protection des data centers d'entreprise. Il est en effet impératif que celles-ci soient actualisées quand les technologies de data centers sont mises à niveau. Si votre système de sécurité IT ne suit pas le rythme des évolutions d'infrastructure ou ne parvient pas à s'y adapter rapidement, voilà une bonne raison de songer à remplacer les techniques de protection de vos data centers par des solutions dédiées.

Ce faisant, souvenez-vous que les data centers sont nés pour constituer une plateforme efficace et ultra-performante contribuant à l'atteinte des objectifs métier. Par conséquent, les solutions de sécurité ne doivent en aucun cas affecter la performance des systèmes utilisés.

Kaspersky Lab propose la solution dédiée « Data Center Security », spécialement conçue pour protéger les data centers d'entreprise contre les cybermenaces les plus sophistiquées, tout en minimisant les effets sur les systèmes des data centers.

Qu'est-ce qu'un data center d'entreprise et pourquoi est-il important de le protéger ?

De nos jours, rares sont les entreprises qui n'ont pas besoin de traiter, stocker et transférer des informations. Toutes ces activités sont aujourd'hui assurées par les data centers d'entreprise, lesquels peuvent être privés ou publics, localisés sur site ou hors site. Dans la plupart des cas cependant, un data center est une entité bien plus complexe dotée d'une infrastructure semi-publique, semi-privée et dispersée géographiquement. Quoi qu'il en soit, un data center moderne élève les activités de l'entreprise à un autre niveau, car il permet à l'infrastructure de s'adapter plus rapidement aux évolutions et de fournir plus efficacement les ressources nécessaires à l'accomplissement des tâches opérationnelles émergentes.

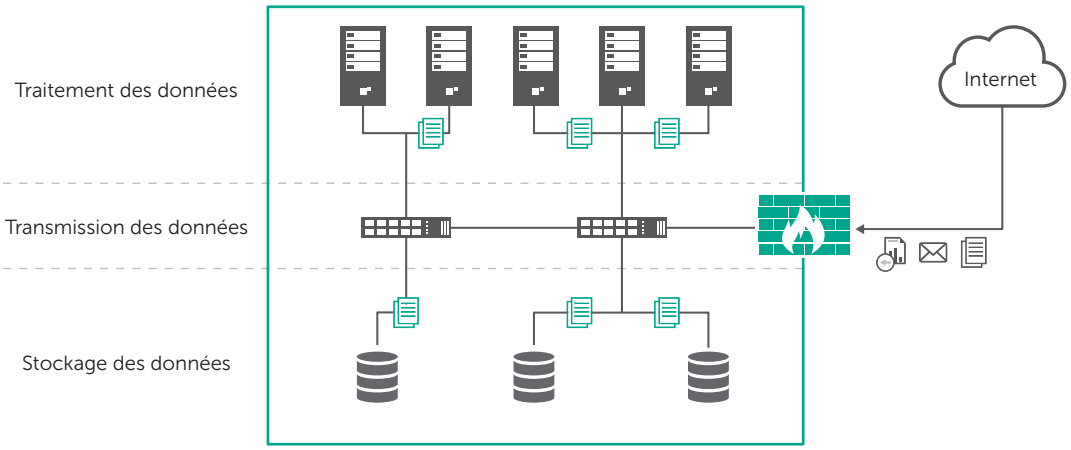


Schéma 1. Architecture complexe d'un data center

« Plus de 75 % des entreprises travaillent déjà avec des software-defined data centers et le taux de pénétration des technologies de virtualisation augmente d'année en année. »

Toutefois, même si les data centers d'entreprise sont construits à l'aide de technologies modernes, l'idéologie sous-jacente à l'organisation de leur infrastructure reste encore largement traditionnelle :

- **Traitement des données** : pour fournir des ressources IT utiles aux applications métier.
- **Stockage des données** : pour stocker les données de l'entreprise.
- **Transmission des données** : pour organiser l'ensemble des communications et des flux de données sans entrave.

Tous ces composants sont essentiels au bon fonctionnement de n'importe quel data center (public, privé ou hybride).

Aujourd'hui, les entreprises considèrent les data centers comme un outil doté d'une infrastructure fiable et de systèmes flexibles avec un niveau de performance et d'efficacité constamment élevé. Elles ont aussi d'autres exigences pour les data centers, à savoir : davantage de ressources, de contrôle, de fiabilité, d'efficacité opérationnelle et de sécurité.

D'après de récentes études et enquêtes, **la protection des infrastructures compte parmi les trois principaux aspects de l'exploitation d'un data center**, tant pour les propriétaires de data centers que pour les grandes entreprises.

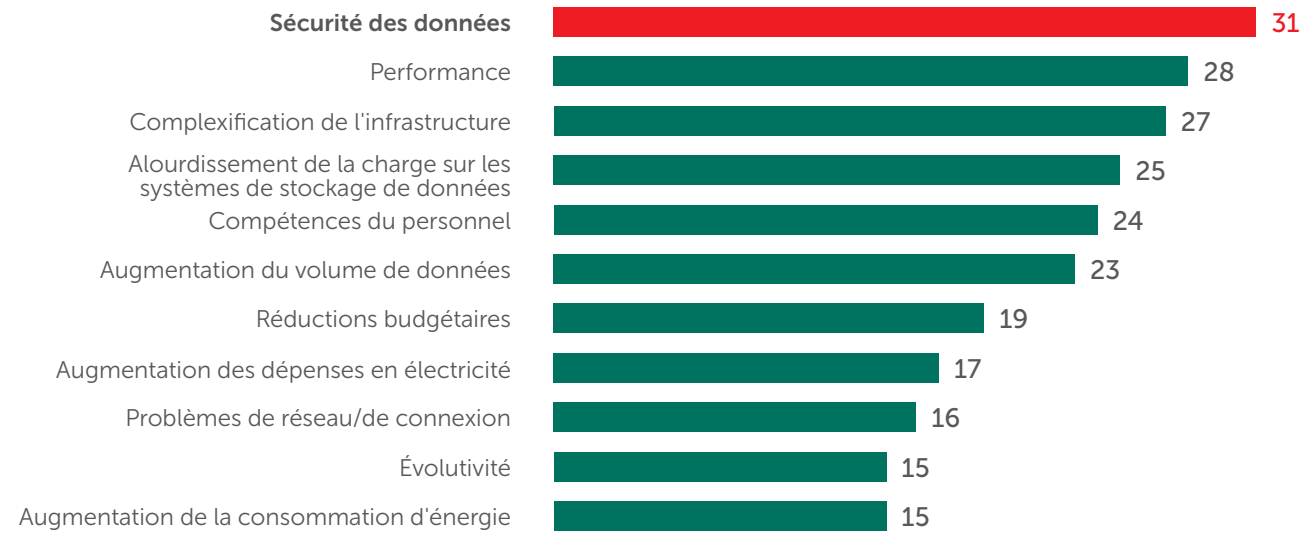


Schéma 2. Principaux problèmes relatifs à la gestion des data centers[1]

Parallèlement au transfert de leurs systèmes métier stratégiques vers des data centers, les entreprises sont de plus en plus conscientes de la nécessité de revoir leur concept de sécurité IT actuel, celui-ci n'étant pas suffisant pour protéger un data center moderne.

Concrètement, les technologies sur lesquelles les data centers modernes reposent s'accompagnent de nouveaux scénarios d'interaction utilisateur et créent des interconnexions supplémentaires entre les composants de l'infrastructure.

« Il est nécessaire de revoir le modèle de sécurité des data centers modernes afin de prendre en compte les technologies qu'utilisent les entreprises pour construire leurs propres data centers. »

Il convient de souligner que si la sécurité est le principal facteur de motivation sous-jacent à la refonte du concept de sécurité IT des data centers modernes, le maintien de la performance des systèmes et un contrôle pratique de l'infrastructure tout entière demeurent des aspects importants pour les dirigeants d'entreprise.

---

http://www.seagate.com/ru/ru/tech-insights/data-center-management-master-ti/

Les principaux éléments à protéger dans votre data center

En termes d'infrastructure, l'environnement d'un data center moderne est une combinaison relativement simple de plusieurs systèmes :

- une infrastructure de traitement des données, qui repose sur une plateforme de virtualisation (VMware vSphere, Microsoft Hyper-V, Citrix XenServer ou KVM) et prend en charge les postes de travail et les serveurs virtuels ;
- une infrastructure de stockage des données d'entreprise, qui regroupe le plus souvent des serveurs de fichiers et des systèmes de stockage de données directement connectés au réseau de l'entreprise ;
- une infrastructure réseau, qui favorise les flux de données et les interactions entre les différents composants de l'infrastructure du data center et intègre notamment des réseaux virtualisés (p. ex. ceux construits à l'aide de la technologie VMware NSX).

Tous ces éléments visent à garantir le bon fonctionnement du data center. Bien sûr, chacun d'entre eux peut voir sa sécurité menacée.

« Les outils utilisés pour protéger un data center doivent "tenir compte" des technologies qu'ils défendent. »

Kaspersky Lab a vocation à fournir des solutions de protection pour chacun de ces éléments, spécialement conçues pour les technologies spécifiques aux data centers.

Data centers modernes : oui à la protection, non à la surcharge

Parfois, les solutions traditionnelles couramment utilisées pour protéger les postes de travail et les serveurs physiques sont également déployées sur les machines virtuelles. Cependant, une fois installée, ce type de solution commence à consommer des ressources, à tel point que les applications métier stratégiques perdent en puissance informatique et ralentissent. Les utilisateurs s'en aperçoivent inévitablement et s'énervent puisqu'ils ne peuvent plus exécuter leurs tâches aussi rapidement et facilement qu'auparavant.

« La virtualisation dans les data centers vise une utilisation efficace des ressources, et les solutions de sécurité IT ne doivent pas aller à l'encontre de cet objectif. »

- Par conséquent, **chaque machine virtuelle** exécute des tâches en soi utiles, mais redondantes au niveau de l'hôte de virtualisation : stockage local et mise à jour des bases de données antivirus, détection des programmes malveillants, autoprotection contre les attaques réseau.
- Il semblerait que cette approche fournisse une protection fiable pour toutes les machines virtuelles. Et pourtant, elle se traduit par une charge excessive pour chacune d'entre elles, qui aboutit en définitive à **une charge supplémentaire considérable sur l'hôte de virtualisation**, entraînant une perte d'efficacité pour l'infrastructure tout entière et ses utilisateurs.
- Lorsque des machines virtuelles téléchargent simultanément des bases de données antivirus ou effectuent simultanément des analyses programmées, la lourde charge sur l'infrastructure du data center provoque des **« blitz de mises à jour »** et des **« blitz d'analyses »**.
- Lorsqu'une machine virtuelle équipée d'une solution antivirus traditionnelle est éteinte, les bases de données antivirus deviennent alors obsolètes, ce qui crée une **« fenêtre de vulnérabilité »** propice à la pénétration de nouveaux programmes malveillants et constituant une menace importante à la sécurité du data center d'entreprise tout entier.
- En outre, l'approche traditionnelle est inutile pour protéger les systèmes de stockage réseau et les serveurs de fichiers, car elle ne garantit pas la **sécurité de toutes les opérations sur fichiers** : en effet, seuls les fichiers téléchargés sur les postes de travail depuis les systèmes de stockage sont protégés ; les dossiers réseau restent vulnérables aux **programmes malveillants de chiffrement (ransomwares y compris).**

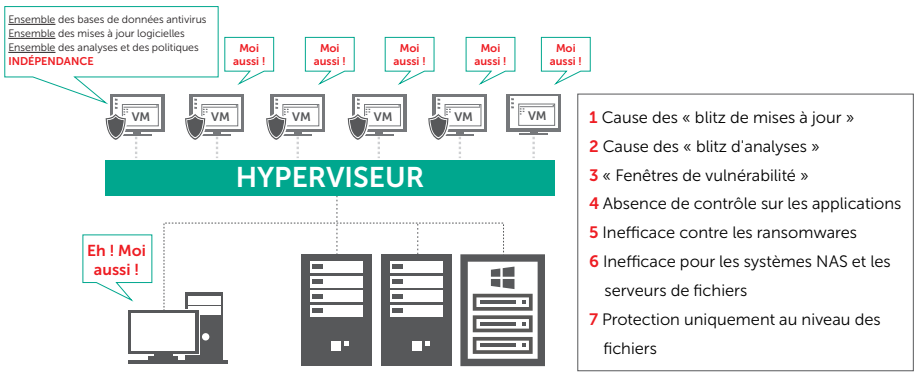


Schéma 3. Inconvénients des solutions de sécurité traditionnelles

Le paysage des menaces dans les data centers modernes

Les solutions traditionnelles destinées à protéger les infrastructures virtuelles peuvent endommager les infrastructures en question. Pas avec des programmes malveillants, mais tout simplement en les ralentissant et en empêchant les systèmes IT de fonctionner normalement et les salariés de l'entreprise d'exécuter leurs tâches.

Des études menées par des leaders de la sécurité IT (Kaspersky Lab y compris) confirment que même les data centers les plus performants ne sont pas à l'abri des menaces actuelles si leurs mesures de sécurité IT sont mal déployées ou inexistantes.

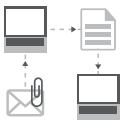
Ce n'est pas que les technologies utilisées dans les data centers modernes sont inadaptées pour résister aux menaces. Bien au contraire, les nouvelles solutions mises en place reposent sur de brillantes idées en matière de sécurité de l'infrastructure : politiques « confiance zéro » pour les pare-feu ou encore méthodologies de microsegmentation, pour n'en citer que quelques-unes. Malgré tout, la défense d'un data center contre les cyberattaques et les programmes malveillants doit s'appuyer sur des solutions dédiées, spécialement conçues pour les systèmes de stockage de données et les environnements virtualisés, et capables de fournir une protection multiniveaux pour le data center tout entier.

L'infrastructure tout entière requiert de nouvelles méthodes de protection

L'infrastructure des software-defined data centers modernes est de plus en plus sophistiquée et regroupe un grand nombre de systèmes destinés à exécuter des tâches multiples. Plus ces tâches sont diversifiées, plus il y a de connexions entre les systèmes et leurs utilisateurs à différents niveaux. Il convient d'assurer une protection fiable et intégrale sans affecter la performance de l'infrastructure et les processus métier qui s'y déroulent. Les technologies les plus avancées doivent être déployées au bon endroit au bon moment, quels que soient la taille et le degré de complexité de l'infrastructure du data center.

Augmentation incontrôlée du nombre de machines virtuelles

Dans les très grandes infrastructures, il est difficile de contrôler l'évolution du nombre de machines virtuelles. Dans la mesure où la virtualisation facilite la création de machines virtuelles à l'aide de modèles et du clonage, la moindre négligence en termes de sécurité ne saurait être tolérée. Pour être plus clair, le fait de reproduire des machines virtuelles non protégées ou infectées peut entraîner des défaillances en masse et de lourdes pertes pour l'entreprise. Votre solution de sécurité doit tenir compte de chacune des activités de votre data center. Plus l'environnement IT est protégé, mieux c'est pour la sécurité de l'entreprise en général.



Cyberattaques réseau

Dans les infrastructures virtualisées, la plupart des interactions réseau passent par des réseaux virtualisés. Dans cette configuration, le trafic réseau et les flux de données atteignent rarement le matériel destiné à protéger l'infrastructure réseau de l'entreprise ou son périmètre. Ainsi, aucun routeur coûteux ni appareil de sécurité ne permet de contrôler totalement votre data center virtualisé. Un système de prévention et de détection des intrusions propre aux réseaux virtuels est indispensable pour un software-defined data center moderne.

Machines virtuelles suspendues

Chaque fois que vous suspendez ou interrompez une machine virtuelle, toute solution traditionnelle de sécurité des terminaux qui y est installée cesse immédiatement de se mettre à jour. Une fois de nouveau active, la machine virtuelle devient le maillon faible de la chaîne de sécurité IT de votre data center moderne. Vous devez par ailleurs garder un œil sur les machines virtuelles éteintes puisqu'elles peuvent contenir des programmes malveillants attendant qu'une machine soit rallumée. Il vous faut une solution fiable, capable d'analyser n'importe quelle machine virtuelle indépendamment de son statut opérationnel.

Menaces contre les « Golden Images » VDI

La virtualisation des postes de travail offre de nombreux avantages et un gain d'efficacité. Il est possible d'utiliser une seule « Golden Image » pour créer des centaines de postes de travail virtualisés en seulement quelques minutes. Cependant, si cette « Golden Image » est endommagée ou infectée, les machines virtuelles ainsi créées peuvent alors représenter un danger, notamment pour les données stratégiques traitées sur ces machines. En outre, il est peu probable que vos administrateurs VDI apprécient que vous leur demandiez d'actualiser les « Golden Images » quotidiennement, simplement parce que vos systèmes de sécurité ont été mis à jour. Pour eux, cette tâche nécessite la mobilisation de ressources considérables. L'architecture de votre solution de sécurité doit être adéquate pour éviter un tel gaspillage des ressources tout en offrant une protection optimale à chaque machine VDI.

Menaces contre les systèmes de stockage de données

Les systèmes de stockage en réseau (NAS) les plus modernes, tout comme les serveurs de fichiers répandus, offrent des capacités étendues en matière de protection des données. Ce dont vous avez besoin, c'est d'une solution supplémentaire spécialement conçue pour les données stratégiques – et plus précisément pour les systèmes de stockage de données – qui n'entrave pas les performances. De plus, vous ne pouvez pas avoir la certitude que les solutions traditionnelles analyseront la totalité des fichiers de votre infrastructure. Quelque chose pourrait rester caché sur les ordinateurs de vos utilisateurs et déjouer vos solutions de protection de terminaux. Il vous faut un outil de sécurité qui s'intègre à l'appareil de stockage lui-même et qui « voit » tous ses mouvements, c'est-à-dire chaque opération sur fichiers, quelle que soit sa provenance.

Consommation excessive de ressources

L'idéologie sous-jacente aux software-defined data centers modernes repose sur le principe d'une amélioration de l'efficacité des systèmes et d'une concentration élevée des ressources IT. Le fait d'installer une solution de sécurité « lourde » crée une charge considérable sur chaque machine virtuelle, entraînant par la même une forte augmentation de l'utilisation des ressources sur les hôtes de virtualisation (hyperviseurs). Aussi, une solution de sécurité inappropriée peut-elle facilement réduire à néant tous les avantages recherchés par une entreprise qui se lance dans la création de son propre software-defined data center moderne.

Protégez votre data center moderne

Kaspersky Lab propose une solution de sécurité dédiée pour les data centers modernes, capable de protéger aussi bien les environnements virtualisés (serveurs et terminaux) que les systèmes de stockage de données d'entreprise. Dès le départ, les composantes de cette solution – Kaspersky Security for Virtualization et Kaspersky Security for Storage – ont été conçues et développées pour s'intégrer aux technologies servant à la création de data centers d'entreprise et favoriser une utilisation optimale des ressources.

L'architecture unique de cette solution a été développée en tenant compte du mode de fonctionnement des data centers modernes : en limitant au maximum l'impact sur la performance des systèmes, en contribuant à maintenir des taux de consolidation élevés et, enfin, en renforçant l'efficacité du projet de création. Cette solution a pour avantage majeur de s'intégrer aux technologies utilisées dans le data center et bénéficie d'une gestion centralisée grâce à une console unique. Les administrateurs système peuvent ainsi mettre en œuvre les politiques de sécurité plus rapidement.

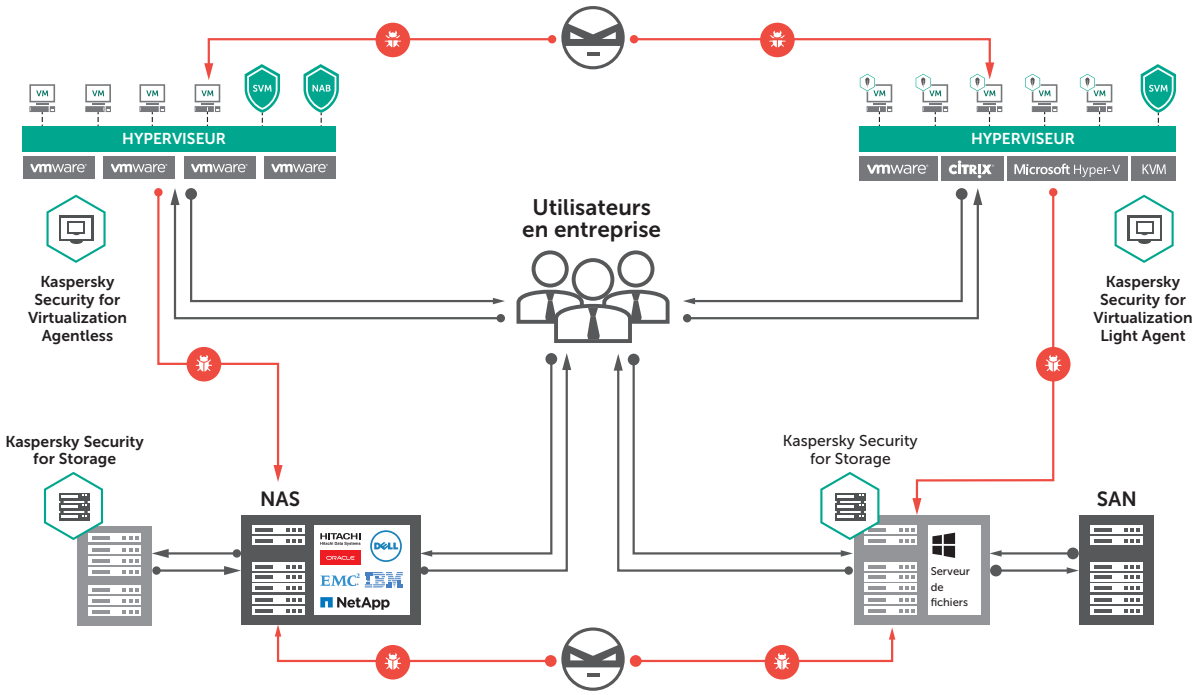


Schéma 4. Architecture de la solution

Kaspersky Security for Virtualization : renforcer la solution VMware NSX pour vSphere

La plateforme VMware vSphere équipée des technologies NSX reproduit le réseau du data center à l'aide d'un modèle défini par logiciel. Ainsi, il est possible de créer ou de reconfigurer la topologie du réseau en seulement quelques secondes, et de mettre en œuvre rapidement une stratégie de sécurité de type « confiance zéro ». Grâce à la solution commune de Kaspersky Lab et VMware, il est plus facile de fournir une protection intégrée à l'infrastructure d'un data center moderne.

La solution **Kaspersky Security for Virtualization Agentless** a été spécialement conçue pour protéger les software-defined data centers reposant sur les technologies VMware. Puisqu'il n'est pas nécessaire d'installer un agent supplémentaire sur les machines virtuelles protégées et que les processus « superflus » pour l'environnement virtualisé sont transférés sur des appareils de sécurité dédiés qui analysent les fichiers et le trafic réseau, la solution n'a qu'un impact minime sur les systèmes d'un software-defined data center et chaque machine virtuelle est protégée dès sa mise en route.

Services VMware NSX intégrés	
Pare-feu distribué	Réseaux virtuels (VXLAN)
Surveillance de l'activité du serveur	VPN (IPSec, SSL L2VPN)
Kaspersky Security for Virtualization	
Protection contre les programmes malveillants	Prévention et détection des intrusions (IDS/IPS) sur un réseau virtuel
Automatisation de la sécurité	Intégration des politiques de sécurité
Intégration des balises de sécurité	Analyse complète de l'infrastructure, même sur les machines virtuelles déconnectées

« Par rapport aux solutions traditionnelles, Kaspersky Security for Virtualization Agentless consomme 40 % moins de mémoire et 80 % moins d'espace disque, des économies qui se traduisent par un fonctionnement efficace et sûr des systèmes. »

La solution interagit avec l'infrastructure VMware grâce à une API dédiée. Ainsi, non seulement chaque machine virtuelle est protégée contre les programmes malveillants et les attaques réseau sont détectées et bloquées, mais la solution est profondément intégrée aux processus à l'œuvre au sein de l'infrastructure.

- Le **déploiement automatique** simplifie considérablement le travail du personnel IT et de sécurité IT grâce à l'automatisation complète des appareils de sécurité sur les hyperviseurs, reposant sur des politiques de sécurité propres à chaque machine virtuelle.
- L'**intégration étroite des politiques de sécurité** implique que chaque machine virtuelle incorpore les fonctionnalités de protection spécifiées par la politique de sécurité IT de l'entreprise.

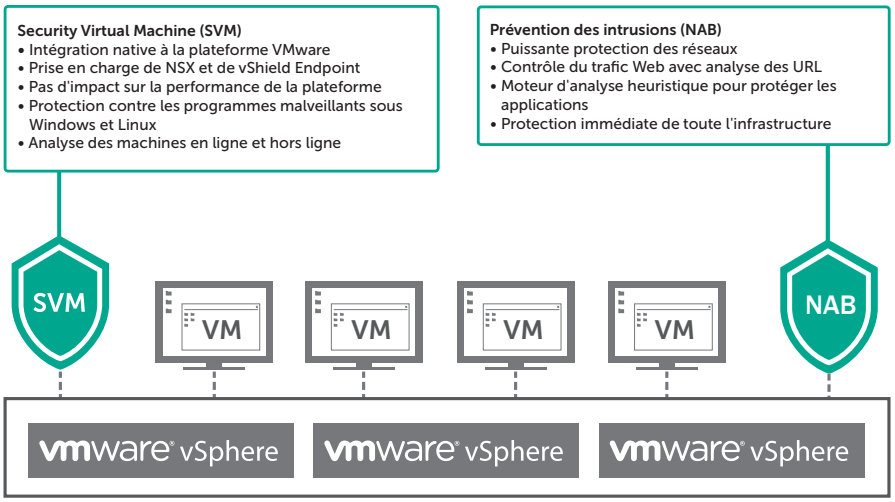


Schéma 5 : Solution de sécurité sans agent

- **L'intégration aux balises de sécurité NSX** élargit la communication entre l'infrastructure et les outils qui la protègent, permettant ainsi au software-defined data center de répondre, de façon complètement automatique et en temps réel, aux incidents de sécurité IT, de prendre des décisions de gestion et de reconfigurer la topologie de son réseau en seulement quelques secondes.
- **Les machines virtuelles en ligne comme hors ligne sont analysées** en mode sans agent, de façon à ce que le data center d'entreprise soit intégralement protégé 24 h/24, 7 j/7.

Dès le départ, l'architecture de la solution a été conçue afin d'avoir un impact quasi nul sur le fonctionnement des serveurs stratégiques de l'entreprise, tout en offrant une protection avancée.

Technologie brevetée d'agent léger

Certains environnements virtualisés hébergés dans des data centers d'entreprise sont dépourvus de protocoles d'intégration reliant l'infrastructure à sa solution de sécurité. Or, il est capital de protéger ces environnements.

En outre, les infrastructures de bureaux virtuels (« VDI ») nécessitent des technologies fournissant une protection fiable à chaque utilisateur, quel que soit son degré de connaissance concernant les menaces et les méthodes de prévention pertinentes.

« L'agent léger contrôle l'exécution des programmes et protège les terminaux virtuels contre les virus de chiffrement et autres menaces. »

Kaspersky Security for Virtualization Light Agent hérite des principes de la solution sans agent tout en offrant des niveaux de protection supplémentaires. Cette solution prend en charge les plateformes de virtualisation les plus répandues (VMware vSphere, Microsoft Hyper-V, Citrix XenServer et KVM) et procure à chaque terminal virtualisé un mix équilibré d'outils et de technologies de protection totalement inédits qui préservent la performance des plateformes VDI (ex. : VMware Horizon et Citrix XenDesktop).

- Protection contre les programmes malveillants et technologies IDS/IPS pour les serveurs virtuels et l'infrastructure VDI
- Protection pour les plateformes VMware, Citrix, Microsoft et KVM
- Protection puissante, mais légère pour les plateformes XenDesktop et Horizon
- Travaille de concert avec votre infrastructure afin qu'elle soit plus performante
- Protection parfaitement équilibrée sans impact sur les performances

Le serveur de protection dédié, baptisé « machine virtuelle de sécurité », effectue des analyses centralisées de l'ensemble des machines virtuelles. Parallèlement, l'agent léger installé sur chaque machine virtuelle permet d'analyser la mémoire et les processus de la machine, en sus des fichiers. Le déploiement de l'agent léger sur les machines VDI favorise l'activation de fonctionnalités de sécurité avancées (contrôle des applications, des appareils, des URL) ainsi que de modules heuristiques qui analysent les e-mails et le trafic Internet. Par ailleurs, les technologies de protection brevetées sur lesquelles repose l'agent léger défendent les terminaux virtuels contre les attaques avancées (virus de chiffrement y compris).

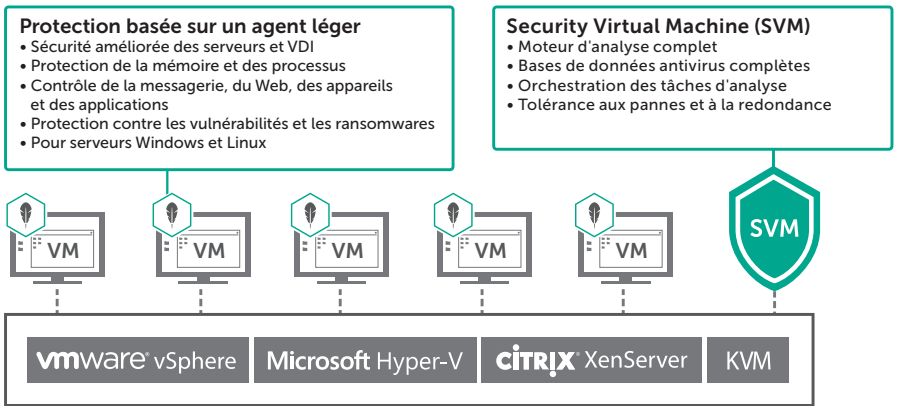


Schéma 6. Principes de fonctionnement de l'agent léger

Protection des systèmes de stockage de données d'entreprise dans les data centers

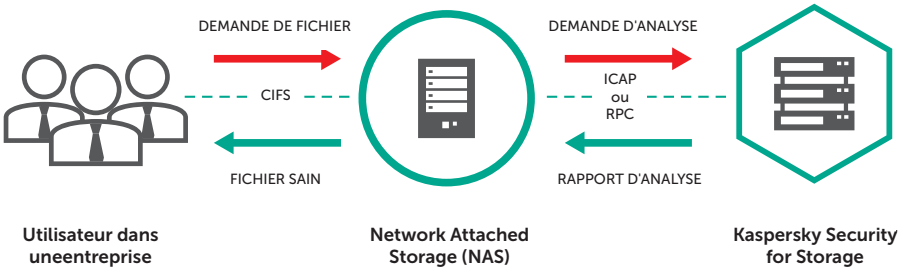
En dépit des technologies de protection les plus avancées pour les terminaux (postes de travail ou serveurs virtualisés), le problème de la protection des données – majoritairement stockées dans des data centers d'entreprise modernes – doit également être traité à l'aide d'outils dédiés.

Kaspersky Lab propose **Kaspersky Security for Storage**, une solution intégrée à de nombreux systèmes de stockage en réseau d'entreprise grâce aux protocoles ICAP et RPC et offrant une protection robuste, ultra-performante et évolutive pour chaque opération sur fichiers. L'architecture de cette solution, associée à un moteur ultra-performant, élimine tout risque potentiel d'une infection de fichiers d'entreprise importants par un programme malveillant.

« Non seulement la solution de sécurité propre aux systèmes de stockage est compatible avec les systèmes de stockage en réseau, mais elle protège également les serveurs de fichiers. »

Peu importe quel utilisateur effectue telle ou telle tâche, toutes les opérations sur fichiers seront traitées par le moteur antivirus de Kaspersky Security for Storage. Ce puissant moteur antivirus développé par Kaspersky Lab analyse chaque fichier ouvert ou modifié à la recherche de toute forme de programme malveillant (virus, vers, chevaux de Troie, etc.). Une analyse heuristique avancée permet d'identifier les nouvelles menaces encore méconnues.

La solution effectue des analyses flexibles et prend notamment en charge les fameuses « zones fiables » (qui ne sont pas nécessairement contrôlées), ainsi que certains formats de fichiers et processus, tels que les copies de sauvegarde.



Résumé

Kaspersky Lab s'appuie sur son moteur de protection primé contre les programmes malveillants pour sécuriser l'intégralité de votre software-defined data center tout en préservant les plus hauts niveaux de performance système. La solution protège l'ensemble des principaux hyperviseurs, y compris dans les environnements VMware vSphere avec NSX, Microsoft Hyper-V, Citrix XenServer et KVM, et s'intègre aux plateformes VDI VMware Horizon et Citrix XenDesktop du secteur.

Outre une sécurité dédiée aux plateformes de virtualisation, nous proposons une solution pour protéger les systèmes NAS (Network Attached Storage) et les serveurs de fichiers d'entreprise, garantissant ainsi la protection de chacune des opérations sur fichiers, indépendamment de leur origine.

La solution Kaspersky Data Center Security redéfinit la manière dont l'infrastructure de votre data center et sa sécurité associent leur puissance pour créer un environnement virtualisé sécurisé et performant. Grâce à ses capacités d'intégration, la solution Kaspersky Data Center Security propose des fonctionnalités de protection avancées pour votre environnement virtualisé en gérant précisément la manière dont vos données sont stockées et leur emplacement, et en protégeant chacune des opérations sur fichiers. Votre data center d'entreprise reste entièrement disponible et sécurisé, 24h/24 et 7j/7.

Kaspersky Lab
pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique :
business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.fr