KASPERSKY lab

PROTECTION DES DATA CENTERS

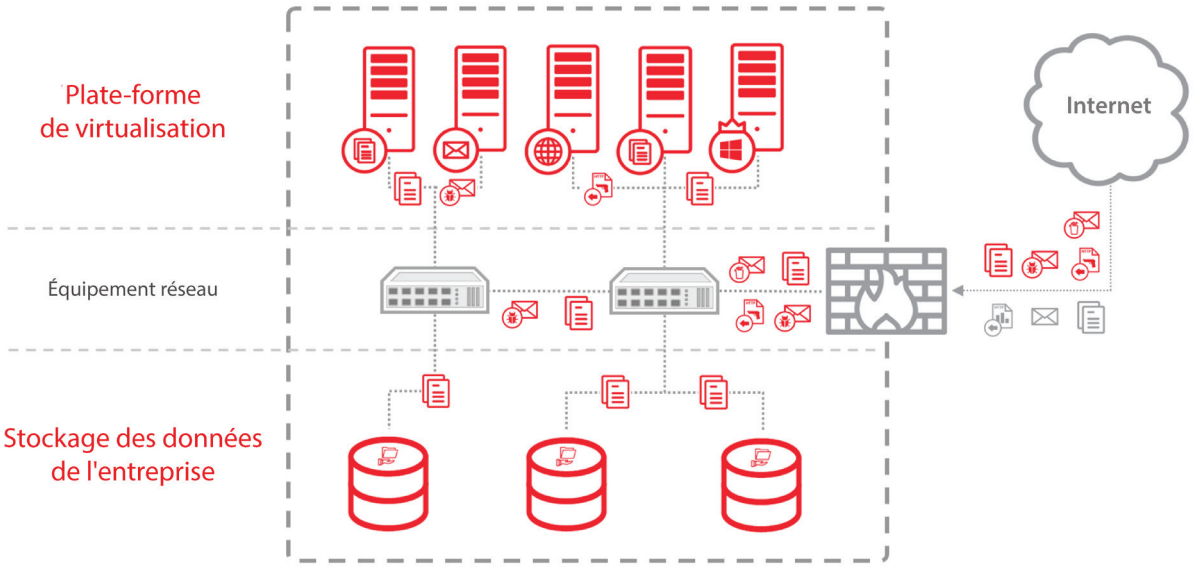
INTRODUCTION

L'administration d'un data center implique la gestion d'une multitude de tâches complexes, dont la sécurité fait bien entendu partie. La sécurité des environnements virtuels et du stockage de données en particulier est d'ailleurs essentielle dans un data center moderne. La sécurisation de ces deux domaines est un véritable défi en soi et, en cas d'échec, les conséquences peuvent s'avérer désagréables. Malheureusement, certains problèmes ne sont pas évidents ou ne sont tout simplement pas pris en compte jusqu'au moment où il est trop tard. Étudions d'un peu plus près ces problèmes et regardons ce qu'il est possible de faire pour les éviter.

SÉCURITÉ DE LA VIRTUALISATION : ERREURS ET CONSÉQUENCES

La virtualisation des différents actifs d'une entreprise est une tendance de plus en plus courante permettant de consommer moins de ressources et de gagner à la fois en flexibilité et en évolutivité. De nombreux scénarios impliquant l'infrastructure virtuelle peuvent d'ailleurs être pris en charge par un data center. Toutefois, étant donné l'étendue des activités entreprises par les data centers, la sécurité des ressources hébergées est bien trop souvent négligée.

Les raisons à cela peuvent être multiples : il est possible que les clients se sentent plus à l'aise en continuant à assurer la sécurité selon leurs propres méthodes habituelles ou qu'ils soient réticents à déléguer la gestion de leur sécurité à un tiers. Il se peut également que les fournisseurs préfèrent ne pas se charger de la sécurité des ressources hébergées.



Un data center fournit à ses clients différents types de ressources, qui doivent toutes être sécurisées.

Ce genre d'attitude peut avoir de graves conséquences. Le fait de « continuer à procéder comme avant » peut donner lieu à l'utilisation d'un ensemble cacophonique de solutions de sécurité indépendantes de la virtualisation, proposées par différents clients et fonctionnant toutes sur le même hébergeur, voire pire, à une absence totale de solution de sécurité. Une telle absence se justifie parfois par des croyances étonnamment tenaces selon lesquelles « les environnements virtuels seraient toujours sûrs » et « les programmes malveillants ne s'exécuteraient pas sur des machines virtuelles ».

Bien entendu, la vérité est tout autre : les machines virtuelles (MV) sont régulièrement les cibles d'attaques, voire présentent un plus grand nombre de failles susceptibles d'être exploitées. Les infrastructures de bureaux virtuels, qui sont généralement utilisées de la même manière que leurs homologues physiques (notamment pour accéder au Web et en matière de dangers que cela comporte), sont particulièrement sensibles aux infections. En un rien de temps, les failles non protégées peuvent déclencher une épidémie de programmes malveillants, risquant d'affecter non seulement le premier client attaqué, mais également tous les autres dont les ressources se trouvent sur le même hébergeur. Une augmentation soudaine de la consommation de ressources déclenchée par une épidémie est susceptible de ralentir les performances, voire de provoquer une panne auprès de l'hébergeur, ce qui est particulièrement ennuyeux pour les clients non infectés concernés.

Il peut également arriver qu'une infrastructure virtualisée spécifique installée dans le data center soit exploitée pour lancer d'autres attaques, une situation susceptible de provoquer le refus de toutes les adresses IP, d'attirer l'attention des autorités et d'entraver entièrement le bon fonctionnement du data center.

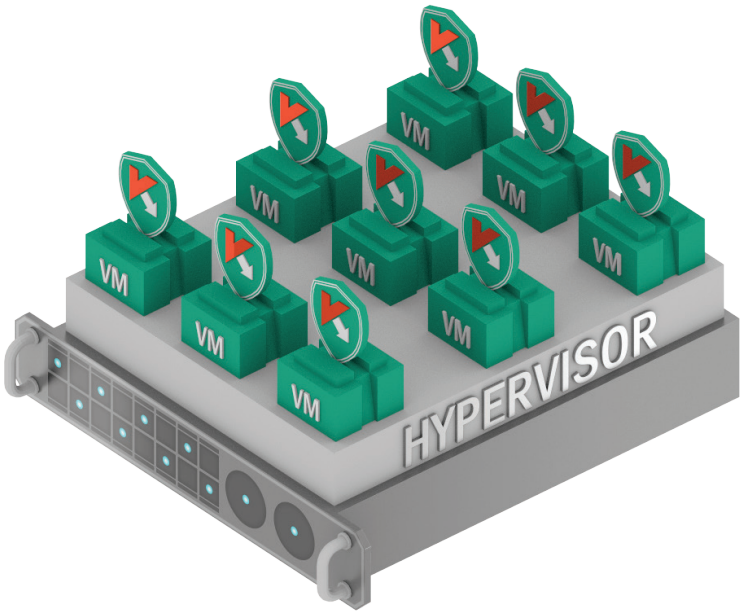
Toutefois, l'installation de solutions de sécurité indépendantes de la virtualisation sur des terminaux virtualisés peut engendrer des problèmes qui lui sont propres.

Il peut s'agir notamment des points suivants :

- Consommation excessive de ressources, où chaque machine protégée comporte un ensemble complet de composants identiques : un moteur d'analyse, une base de données de signatures locale, un système de prévention des intrusions basé sur l'hébergeur, etc. De plus, en cas d'utilisation de flux de données sur les menaces basés dans le cloud, chacun d'entre eux aura besoin de sa propre bande passante.
- Augmentations soudaines et imprévisibles de la consommation de ressources, appelées « tempêtes », induites par l'exécution simultanée de tâches similaires, telles que la mise à jour ou l'analyse des fichiers du système, sur plusieurs machines virtuelles. Cette situation peut entraîner de sérieux décalages, voir un déni de service sur l'ensemble de la machine hôte.
- Attaques de panique : les épidémies de programmes malveillants induisent souvent un passage en mode « paranoïaque », qui déclenche des analyses non planifiées, augmente l'étendue des analyses, etc. La baisse des performances qui en découle peut affecter toutes les machines virtuelles hébergées sur le même serveur.

- « Brèches instantanées de la sécurité » : certaines machines virtuelles peuvent rester inactives jusqu'à ce que leurs services soient nécessaires. Inactives, elles ne peuvent pas être mises à jour (les correctifs des failles et les mises à jour de la solution de sécurité ne peuvent donc pas être appliqués). Ainsi, dès qu'elle est activée, la machine est vulnérable tant qu'elle n'a pas été mise à jour, ce qui est suffisant pour contracter une infection.
- Incompatibilité. Bien que les machines virtuelles soient similaires à leurs homologues physiques en bien des aspects, elles comportent quelques différences. Les solutions de sécurité indépendantes de la virtualisation ne sont pas conçues pour fonctionner dans le cas, par exemple, de migration des machines virtuelles ou des supports de stockage virtuels attribués de manière dynamique, ce qui peut créer des problèmes ou des dysfonctionnements bien plus graves.

Il est essentiel de reconnaître que les conséquences énumérées ici relèvent en fin de compte de la responsabilité du prestataire de services ; le fait que vous n'ayez aucun contrôle sur les ressources hébergées ne constitue pas une défense, ce qui est d'autant plus vrai qu'il EXISTE réellement des moyens de prendre le contrôle dans un environnement virtualisé.



1. Cause des « tempêtes de mises à jour »
2. Cause des « tempêtes d'analyses »
3. « Brèches instantanées »
4. Consommation excessive de ressources
5. Plus faible densité des machines virtuelles
6. Absence de sécurité pour les ressources du réseau

L'utilisation d'une protection indépendante de la virtualisation engendre de nombreux problèmes, à commencer par l'utilisation inefficace des ressources.

La réponse consiste à avoir recours à des solutions de sécurité spécialisées, conçues tout particulièrement autour de la virtualisation.

UTILISEZ UNE PROTECTION CONÇUE À PARTIR DE VOS PROPRES BESOINS

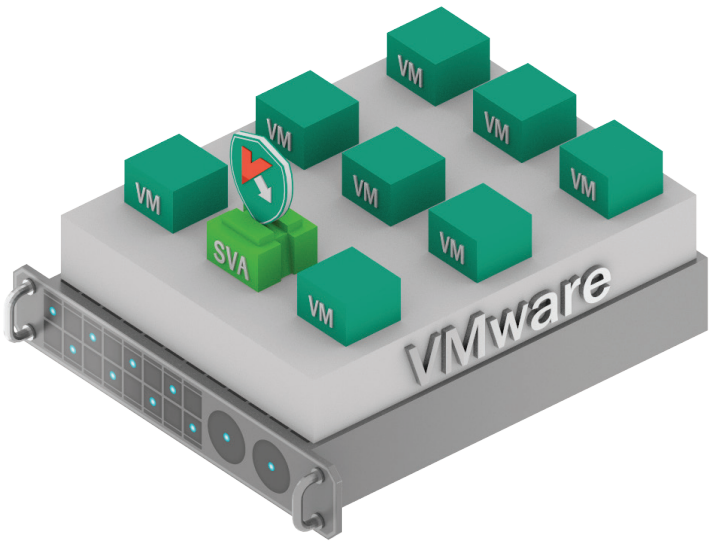
Kaspersky Security for Virtualization a été conçue en prenant en compte les spécificités de l'infrastructure virtuelle. Nous l'avons d'ailleurs développée de sorte qu'elle s'intègre naturellement dans ces environnements et qu'elle évite ainsi les problèmes causés par des solutions inappropriées, inefficaces ou inadaptées.

Premièrement, nous avons supprimé toute redondance au niveau des composants de chaque machine virtuelle. Une machine virtuelle dédiée, appelée **appliance virtuelle de sécurité**, est équipée de façon centralisée du moteur d'analyse et de la base de données de sécurité, ce qui permet de protéger chaque machine virtuelle fonctionnant avec le même hyperviseur. Il est ainsi possible d'appliquer les mises à jour en permanence et d'utiliser des méthodes de planification intelligentes afin de gérer les analyses et d'éviter les tempêtes.

Bien entendu, cette appliance virtuelle de sécurité doit pouvoir atteindre chaque machine virtuelle protégée. Kaspersky Security for Virtualization permet d'y parvenir de deux manières :

Protection sans agent

Cette option ne fonctionne que dans les environnements VMware. Comme son nom l'indique, l'installation d'un agent logiciel sur la machine virtuelle n'est pas nécessaire ; celui-ci est remplacé par la technologie native vShield. Avec une protection sans agent, **chaque machine virtuelle est automatiquement protégée**, dès son activation, tandis qu'une appliance virtuelle de sécurité supplémentaire propose un **système de prévention des intrusions** sur le réseau.



La solution sans agent permet de bénéficier d'une protection instantanée sans avoir à effectuer d'installation sur les machines virtuelles

Cette protection sans agent est idéale lorsqu'il s'agit de protéger des clients susceptibles de laisser des logiciels étrangers accéder à leurs machines ou n'exécutant qu'un ensemble d'applications strictement défini. Lorsque les clients ne souhaitent utiliser AUCUNE solution de sécurité, cette mesure peut représenter le seul moyen d'éviter d'avoir à colmater les failles de sécurité.

Toutefois, il convient de prendre en compte certains points.
La technologie sans agent ne permet pas à la solution de sécurité d'étudier les processus exécutés dans la mémoire de la machine virtuelle : avec la technologie vShield, il n'est possible d'accéder qu'aux systèmes de fichiers des machines, ce qui limite l'efficacité de la protection contre les programmes malveillants sophistiqués (tels que les variantes sans corps).

Il est également impossible de mettre en œuvre des niveaux de sécurité proactifs supplémentaires, tels que le contrôle du Web, des appareils et des applications. Ainsi, dans certains cas, par exemple dans le cadre du remplacement de plus en plus fréquent des postes de travail physiques par des infrastructures de bureaux virtuels, nous vous recommandons d'utiliser l'autre option proposée par Kaspersky Security for Virtualization : la protection basée sur un agent léger.

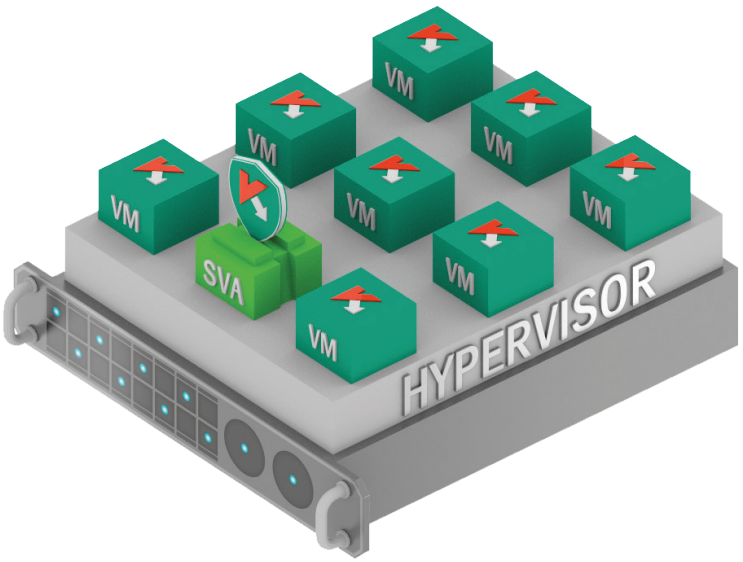
Protection basée sur un agent léger

Contrairement à la sécurité sans agent, cette option ne repose pas sur un **niveau intermédiaire dépendant de la plateforme**. Par conséquent, elle peut fonctionner avec une large palette d'hyperviseurs, dont Microsoft Hyper-V et Citrix, qui viennent s'ajouter à la liste des hyperviseurs pris en charge. Cette méthode est possible à condition d'utiliser un **agent logiciel léger** déployé sur la machine virtuelle protégée. La présence de ces agents permet non seulement au moteur de lutte contre les programmes malveillants de l'appliance virtuelle de sécurité d'atteindre les machines protégées, mais également de bénéficier d'un plus grand nombre de technologies de protection. Il est ainsi possible de renforcer le niveau de sécurité de façon à qu'il atteigne **celui d'une solution de protection totale des terminaux**, telle que Kaspersky Endpoint Security for Business.

Kaspersky Security for Virtualization | Light Agent présente entre autres les avantages suivants :

- Contrôles des processus exécutés dans la mémoire des machines virtuelles à l'aide de mécanismes comportementaux avancés
- Réduction des failles d'exploitation grâce à la technologie de prévention automatique des vulnérabilités
- Programme antivirus Web avec dispositif antiphishing compatible avec le cloud
- Ensemble complet de contrôles de sécurité, qui permet de définir explicitement les applications, les ressources Web, voire les appareils externes autorisés sur chaque machine virtuelle.
- Protection avancée du réseau, avec mécanismes de blocage des attaques du réseau, équipements et pare-feu avancés, qui permet de garantir la sécurité du fonctionnement de chaque machine au sein des réseaux virtualisés.

Malgré toutes ces fonctionnalités, l'agent demeure très léger : l'appliance virtuelle de sécurité se charge toujours des mises à jour et de la gestion des analyses en supprimant les redondances et en assurant un minimum de sécurité au niveau de l'activité de l'agent sur la machine virtuelle.

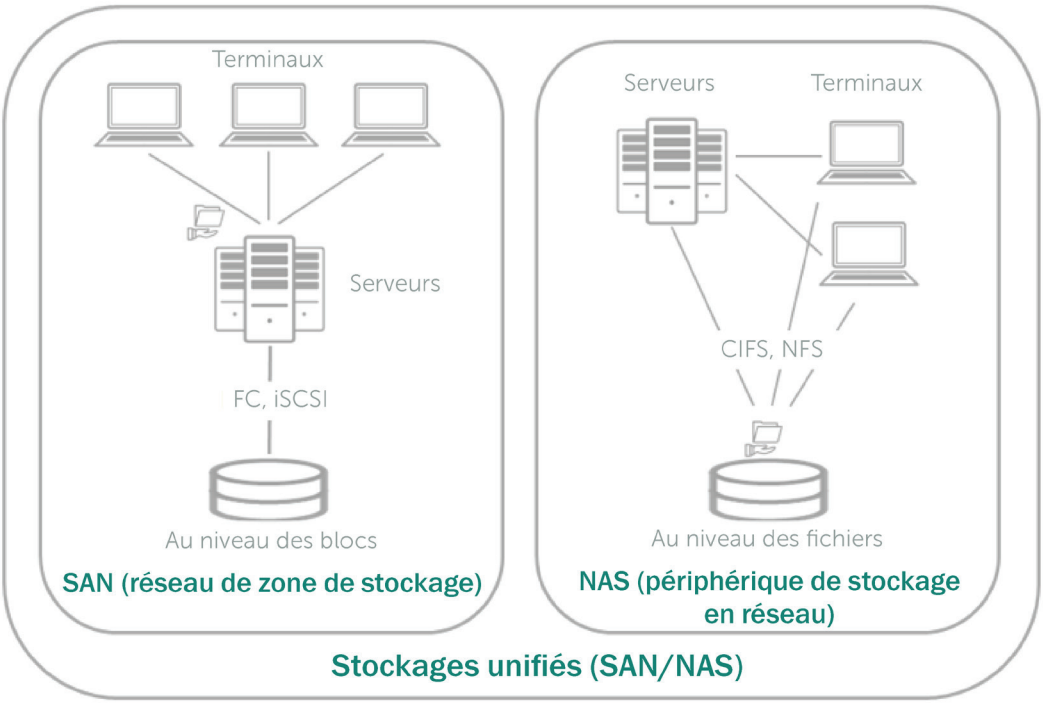


Une solution avec agents légers permet de bénéficier d'une protection avancée en utilisant des applications légères et en offrant de de la visibilité sur les machines virtuelles. Ces applications peuvent être pré-installées sur les images des machines virtuelles.

Pour les cas impliquant des risques plus sérieux et des surfaces d'attaque potentielle plus importantes (par exemple, des bureaux virtualisés avec accès total à Internet), ce type de protection sur plusieurs niveaux est idéal, et pas seulement parce que la probabilité d'une attaque est plus élevée. Étant donné que les réseaux virtualisés sont bien plus efficaces, l'infection peut se propager à la vitesse de l'éclair, permettant ainsi aux attaquants de prendre le contrôle sur une infrastructure mal protégée en un rien de temps. D'autre part, une infrastructure virtuelle bien protégée représente une cible moins attirante, même pour les auteurs d'attaques ciblées à la recherche de gains faciles.

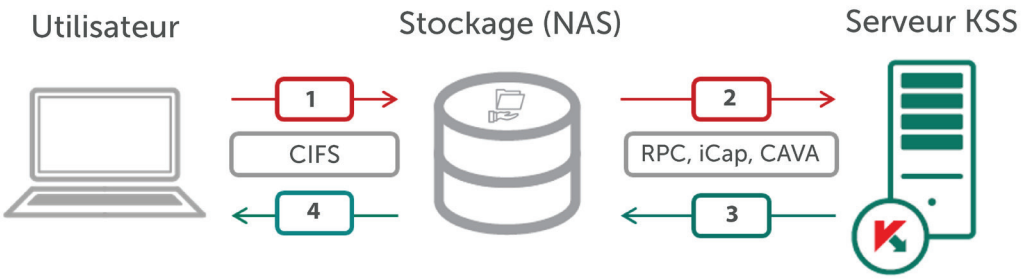
SÉCURISATION DU STOCKAGE DE DONNÉES : VIRTUALISATION OU NON ?

Lorsqu'il s'agit de sécurité du data center, il convient de bien étudier les supports de stockage de données. D'importantes quantités de données sont stockées, mises à jour et partagées, ce qui représente une source de danger potentiel pour des centaines d'utilisateurs en cas de négligence ou de mauvaise intention de l'un d'entre eux. Il convient également de garder à l'esprit que les utilisateurs peuvent se trouver en dehors du périmètre protégé : le data center n'a aucun contrôle ni aucune information sur leur niveau de sécurité. Il est donc recommandé de prendre des mesures afin de sécuriser différents types de support de stockage de données, notamment s'ils ne sont pas tous virtualisés et protégés par une solution de sécurité spécifique pour la virtualisation.



Quel que soit le support de stockage, celui-ci doit être protégé

Tandis que la protection des **réseaux de zone de stockage (SAN)** est plutôt simple (étant donné qu'il n'est possible d'y accéder qu'à partir de serveurs), la sécurisation des **périphériques de stockage en réseau (NAS)**, auxquels les utilisateurs du réseau accèdent directement, s'avère plus complexe.



Il est plus difficile de protéger un support de stockage NAS qu'un réseau SAN

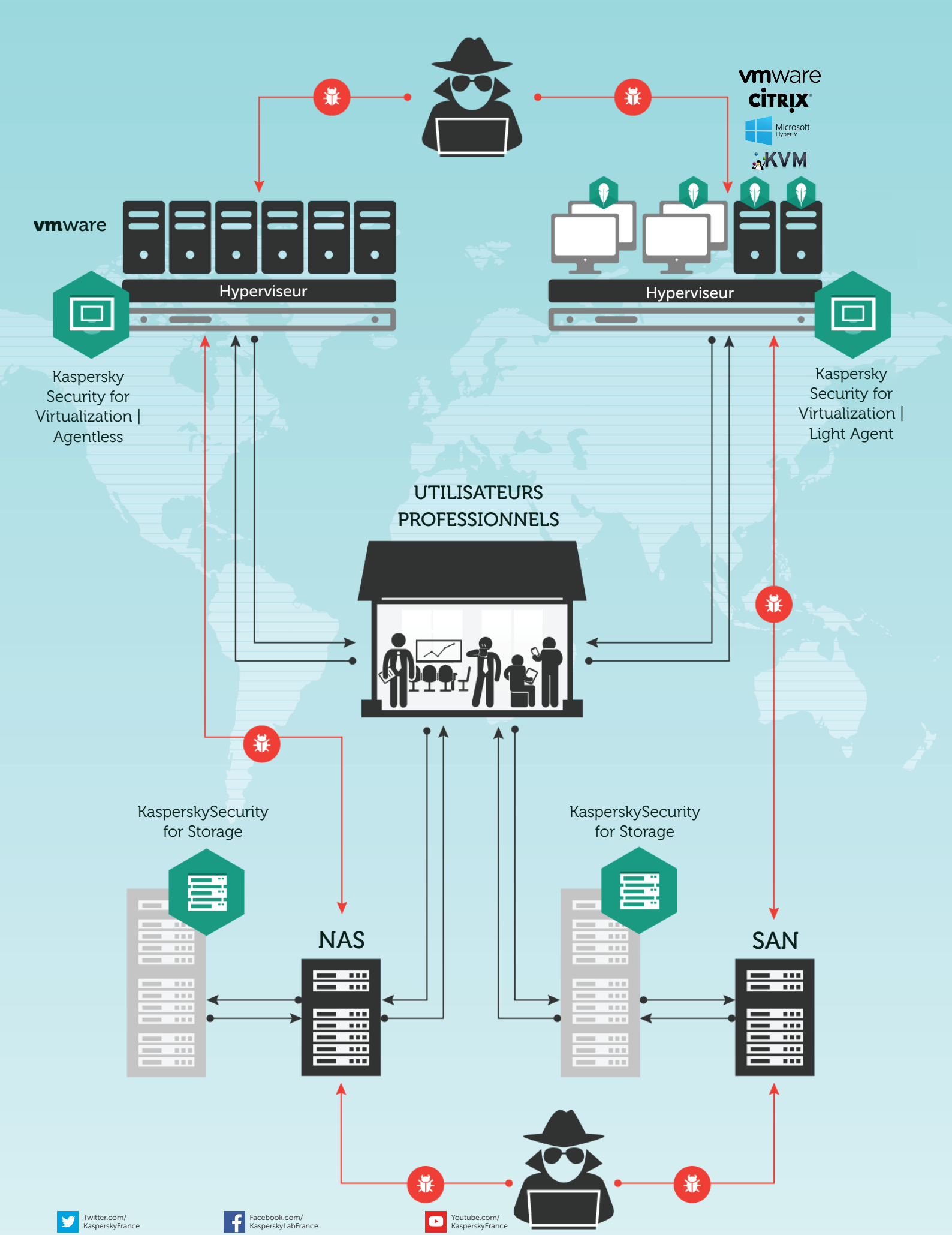
Fort heureusement, il existe des solutions de sécurité spécialisées permettant de les protéger tous les deux ; Kaspersky Security for Storage en est un bon exemple. Les ressources du réseau SAN sont sécurisées, tout comme les systèmes de fichiers habituels, excepté que chaque objet transféré vers (ou demandé par) un support de stockage NAS est tout d'abord vérifié par la solution de Kaspersky Lab. En fonction du verdict de la solution, le support NAS peut accorder ou refuser la permission de terminer l'action demandée. Afin de gérer des flux de données plus importants, plusieurs instances de la solution peuvent être déployées, l'équilibrage des charges étant pris en charge par le support NAS.

UNE CONSOLE DE GESTION CENTRALISEE

Avec l'augmentation du nombre de cyberattaques modernes et de leur niveau de sophistication, il est essentiel que la personne en charge de la sécurité du data center dispose d'une vue d'ensemble de l'infrastructure, qu'elle puisse prendre connaissance des menaces rapidement et y remédier efficacement. À ce niveau, les solutions Kaspersky Lab bénéficient d'un avantage supplémentaire : l'ensemble de la sécurité est surveillée et gérée à partir d'une console flexible et d'un seul et même écran : Kaspersky Security Center. Par ailleurs, un accès disponible en option en fonction des rôles vous permet de donner à vos clients la possibilité de gérer l'état de leur propre sécurité si nécessaire, sans compromettre la sécurité globale du data center.

CONCLUSION

Que vous ayez affaire à des ressources physiques ou virtualisées, la solution de Kaspersky Lab pour data center (qui fait partie de notre plateforme de sécurité de l'entreprise) permet de faire de la sécurité informatique une offre intéressante (et rentable) au sein de votre portefeuille de services pour data center. Mais une chose est sûre : si vous voulez surmonter les prochaines tempêtes, n'hésitez pas à prendre en main la sécurité de votre data center.



Twitter.com/KasperskyFrance

Facebook.com/KasperskyLabFrance

Youtube.com/KasperskyFrance

Kaspersky Lab France
www.kaspersky.fr

Tout savoir sur la sécurité sur Internet :
www.securelist.fr

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab