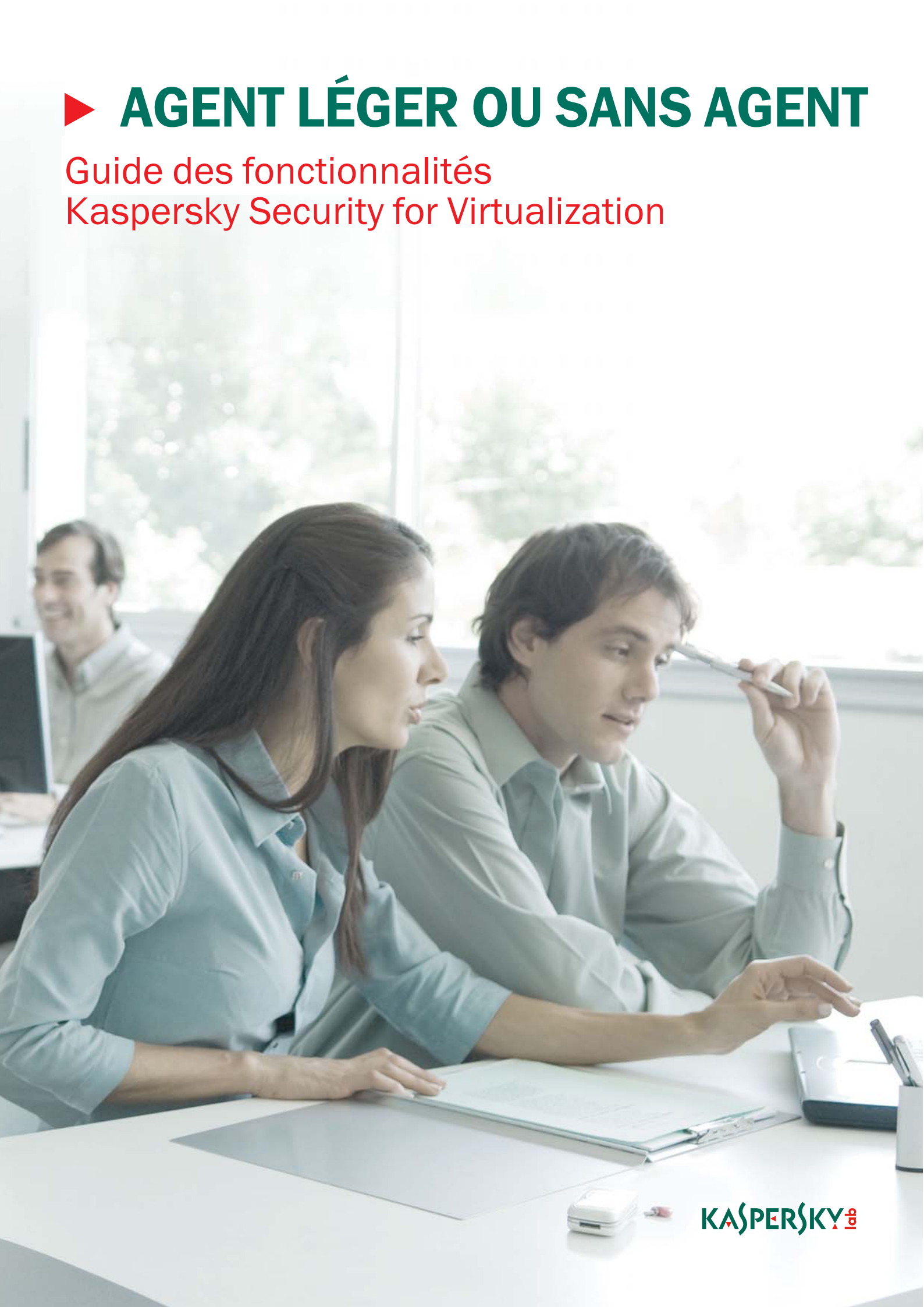
AGENT LÉGER OU SANS AGENT

Guide des fonctionnalités
Kaspersky Security for Virtualization



KASPERSKY lab

Avec la généralisation de la virtualisation, le besoin de solutions de sécurité est une évidence. Bien qu'ils soient aussi vulnérables aux cyber-attaques que tout autre système physique, les environnements virtuels présentent des spécificités dont il convient de tenir compte lors de la recherche d'une solution de sécurité.

Si elles offrent un certain niveau de protection, les solutions standard qui ne sont pas conçues spécifiquement pour des environnements virtuels peuvent néanmoins présenter les problèmes suivants :

1) **Une utilisation excessive des ressources** en raison de la réplication des bases de données de signatures et des moteurs de protection contre les programmes malveillants actifs sur chaque machine virtuelle protégée (VM).
2) **Les « blitz »**, qui se présentent sous la forme de mises à jour simultanées de base de données et/ou de processus d'analyse des programmes malveillants sur plusieurs machines virtuelles. Résultat : une augmentation importante au niveau de la consommation des ressources avec effet boule de neige et une détérioration significative des performances pouvant entraîner un déni de service. Les efforts nécessaires à la planification des processus pour atténuer le problème génèrent des « périodes de vulnérabilité », à savoir des moments pendant lesquels la machine virtuelle reste exposée aux attaques en raison du report des analyses de détection des programmes malveillants.
3) **Les clichés instantanés**. Comme il n'est pas possible de mettre à jour les bases de données de signatures sur des machines virtuelles inactives, la machine virtuelle est vulnérable face aux attaques, de son démarrage jusqu'à la fin du processus de mise à jour.
4) **Les incompatibilités.** En l'absence de solutions standard pour traiter les fonctions spécifiques à la virtualisation, telles que la migration des machines virtuelles ou le stockage non persistant, leur utilisation peut engendrer une instabilité voire un blocage du système.

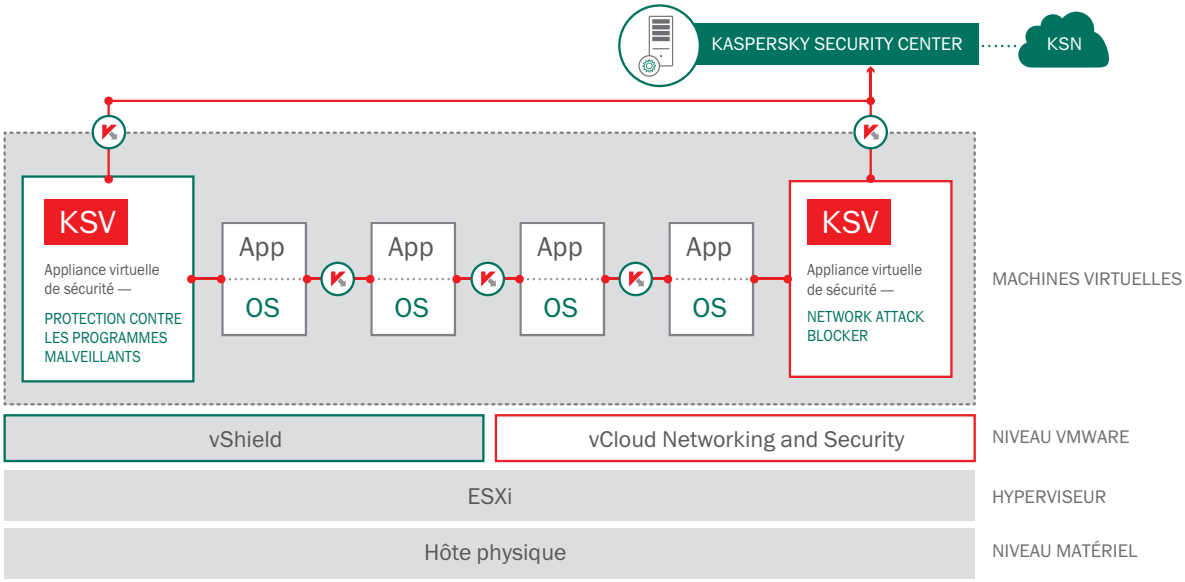
Conscient de l'importance de la sécurité des systèmes virtuels et des fonctions uniques offertes par la virtualisation, le leader du marché VMware a développé la technologie vShield, une couche défensive spécifique pour sa plate-forme vSphere. Cette couche crée un espace de sécurité intégré qui englobe l'ensemble des ressources virtualisées et permet un accès à la fois simple et efficace aux solutions de sécurité conçues de façon appropriée. Parmi les avantages évidents de cette approche figure notamment le fait qu'il soit désormais possible d'offrir aux terminaux virtualisés une protection « sans agent ». Il ne suffit que d'une seule appliance virtuelle de sécurité, à savoir une machine virtuelle spécialisée équipée d'un moteur de détection des programmes malveillants, ainsi que de bases de données de signatures pour soulager les différentes machines virtuelles de ce problème et réduire ainsi nettement l'utilisation des ressources. Les solutions de sécurité compatibles vShield capables d'exploiter pleinement l'ensemble des fonctions proposées par l'environnement VMware offrent de nombreux avantages aux utilisateurs grâce à cette approche.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless est spécifiquement conçu pour exploiter tous les avantages de la technologie vShield. Reposant sur la technologie primée du moteur de protection contre les programmes malveillants de Kaspersky Lab, une appliance virtuelle de sécurité conçue pour un déploiement prêt à l'emploi offre des taux de détection de premier ordre. Le support du service Kaspersky Security Network (KSN) basé sur le cloud permet les temps de réaction les plus rapides tout en réduisant sensiblement le nombre de faux positifs. Il est également possible de faire appel à une deuxième appliance afin d'exploiter la technologie Network Attack Blocker de Kaspersky Lab conjointement avec le composant de sécurité et réseau vCloud de VMware.

Cependant, une approche « sans agent » présente des inconvénients.

Premièrement, VMware est le seul fournisseur de couche de sécurité intermédiaire ; pour les autres plates-formes, la solution de sécurité doit donc accéder aux différentes machines virtuelles d'une autre façon. Deuxièmement, vShield ne propose aucun accès aux processus internes des machines virtuelles, ce qui réduit fortement la capacité d'une solution à offrir à ce niveau une protection renforcée contre des programmes malveillants élaborés.



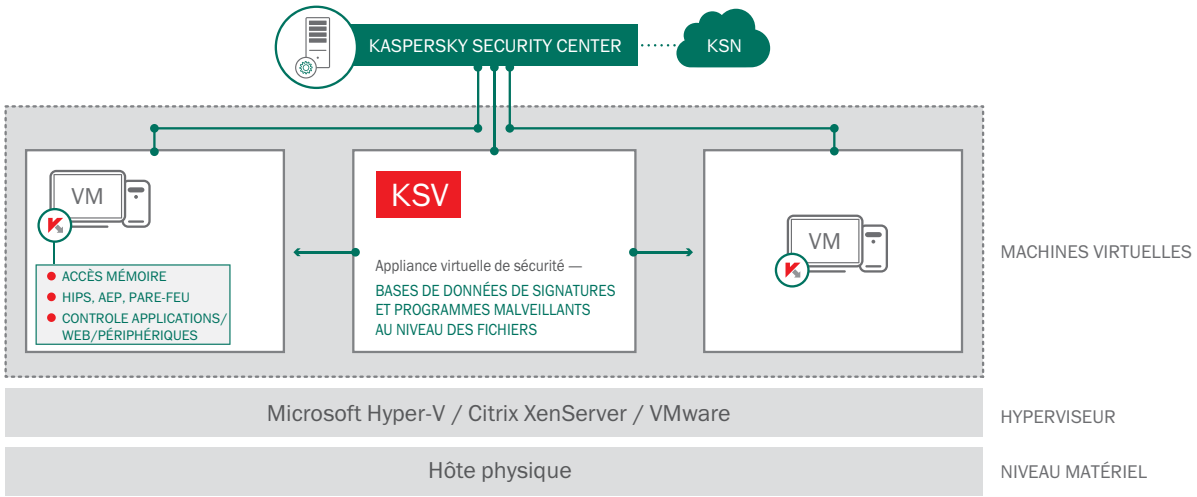
Pour contourner ces restrictions, une autre approche consistant à déployer, parallèlement à l'appliance, une application compacte sur la machine virtuelle protégée a vu le jour. Cette application est connue sous le nom d'« agent léger ». Dans la mesure où le moteur d'analyse des fichiers et les bases de données sont centralisés, cette application a un impact plus limité sur la mémoire de la machine virtuelle que la solution complète basée sur un agent. Par ailleurs, l'accès qu'elle permet ne se limite pas au seul système de fichiers de la machine virtuelle mais couvre également sa mémoire et ses processus internes. Par conséquent, il est possible de faire appel à d'autres techniques de sécurité plus avancées.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Kaspersky Security for Virtualization | Light Agent est destiné aux trois plates-formes de virtualisation les plus populaires : Citrix, Microsoft Hyper-V et VMware. Le moteur de détection des programmes malveillants et les bases de données de signatures résident sur une appliance virtuelle de sécurité, comme dans le cadre de la technologie sans agent, ce qui libère les ressources pour le déploiement de machines virtuelles supplémentaires et optimise les ratios de consolidation. Grâce à un agent léger qui fonctionne au sein de chaque système d'exploitation invité, il devient également possible de faire appel à la plupart des technologies avancées disponibles pour les machines physiques via **Kaspersky Endpoint Security for Business**. Une gamme complète de contrôles des terminaux peut être déployée en même temps qu'un système HIPS, un pare-feu propriétaire et des outils de gestion des systèmes. Cette solution permet de créer un puissant périmètre défensif multiniveau, capable de traiter les programmes malveillants les plus sophistiqués ainsi que les menaces « zero-day ».

Naturellement, même si elle offre un niveau de protection supérieur, la solution proposant un **agent léger** semble « plus lourde » que sa contrepartie fonctionnant **sans agent** tout en exigeant une plus grande attention lors du déploiement de nouvelles machines virtuelles. Ces problèmes ne sont toutefois pas évidents à première vue.

Pour mieux les comprendre, il convient d'observer de plus près le fonctionnement des solutions **sans agent** et avec **agent léger**, ainsi que les menaces qu'elles sont censées contrer.



MENACES ET FONCTIONNALITÉS

Les machines virtuelles sont aussi vulnérables que leur équivalent physique, voire davantage : sur des réseaux virtuels ultra-rapides, la propagation des virus peut être dévastatrice. Il est donc important d'identifier les faiblesses en matière de sécurité dans votre infrastructure virtuelle et de déployer des mesures à la hauteur des menaces potentielles. Vous trouverez ci-dessous une analyse des menaces qui pèsent sur les systèmes virtuels et des technologies pour les contrer.

EXÉCUTABLES MALVEILLANTS

Les pièces jointes des courriers électroniques, les logiciels de divertissement ou d'autres exécutables peuvent être infectés par des codes malveillants, il est donc essentiel de posséder un logiciel de protection pour traiter ces menaces de base. Le moteur de protection contre les programmes malveillants représente la technologie principale des solutions **sans agent** et avec **agent léger** de **Kaspersky Security for Virtualization**, même s'ils accèdent à chaque fois différemment aux systèmes de fichiers de la machine virtuelle protégée.

Pour empêcher des agents malveillants de nuire à vos ressources virtualisées, il est également possible de faire appel au contrôle des applications au moyen d'une liste blanche dynamique. Pour intercepter les programmes malveillants et bloquer leur propagation, il convient de n'autoriser que l'exécution de logiciels reconnus et sécurisés. Kaspersky Security for Virtualization | Light Agent permet le contrôle des applications sur les machines virtuelles, bien que Kaspersky Security for Virtualization | Agentless, reposant sur la technologie vShield, ne prenne pas en charge les contrôles de terminaux.

PROGRAMMES MALVEILLANTS SANS CORPS

Certains programmes malveillants n'ont pas de « corps », ce qui signifie qu'ils sont introuvables dans le système de fichiers. Diffusé à l'aide d'un exécutable lancé précédemment ou injecté via une faille d'exploitation, ce type de programme ne peut pas être détecté par un logiciel traditionnel de protection contre les programmes malveillants. Il convient, dans ce cas, de prendre des mesures de protection avancées, capables de surveiller les processus en mémoire et de bloquer immédiatement les programmes dont le comportement semble suspect ou dangereux. **Kaspersky Security for Virtualization | Light Agent** repose sur un ensemble de technologies capables de bloquer les intrusions dans la mémoire de la machine virtuelle. Ces technologies sont les suivantes :

- System Watcher, qui surveille le comportement des programmes et effectue un suivi des événements du système. Cette fonction est prise en charge par :
- Les signatures de flux de comportement (BSS), qui identifient les schémas comportementaux caractéristiques de l'activité des programmes malveillants.
- Le contrôle des privilèges, qui empêche l'application d'apporter des modifications non sollicitées, dont l'injection de processus.

Ces outils permettent au système HIPS de suivre et de bloquer les processus malveillants évoluant dans la mémoire de la machine virtuelle.

Kaspersky Security for Virtualization | Agentless ne peut suivre que les changements au niveau du système de fichiers en raison de restrictions propres à l'API vShield.

EXPLOITATION DE FAILLES

L'exploitation des failles identifiées dans les composants du système et les applications les plus connues compte parmi les stratégies d'attaque les plus efficaces. S'il est possible de contrer ces intrusions à l'aide des technologies évoquées plus haut, le programme affecté peut disposer d'un niveau de privilège élevé, ce qui limite le contrôle de ses activités. La méthode la plus efficace pour faire face à cette menace consiste à empêcher les failles d'accomplir leur mission principale, à savoir exploiter en priorité les vulnérabilités.

Il convient, dans ce cas, d'identifier l'ordre d'exécution des actions propres aux failles en utilisant la technologie AEP de prévention automatique des failles d'exploitation de Kaspersky Lab. L'efficacité de cette technologie a été confirmée par une batterie de tests indépendants réalisés par l'institut MRG Effitas. Ces tests ont révélé que la technologie de prévention automatique des failles d'exploitation de Kaspersky Lab offrait une efficacité de 100 % contre les attaques à partir de failles, même en cas de désactivation de tous les autres composants de protection. Les failles « zero-day » inconnues ne font pas exception à la règle et sont également bloquées par cette technologie proactive.

Kaspersky Security for Virtualization | Light Agent est équipé de cette fonction avancée particulièrement utile dans les infrastructures de postes de travail virtuels utilisées pour remplacer les postes de travail physiques et exposées aux risques beaucoup plus élevés d'infections intempestives.

Kaspersky Security for Virtualization | Agentless repose sur la technologie vShield, qui ne propose pas les mêmes fonctions que Kaspersky AEP.

ROOTKITS

Les programmes malveillants sophistiqués sont souvent capables de se dissimuler et d'empêcher les logiciels traditionnels de protection contre les programmes malveillants de les détecter à l'aide de « bootkits » et de « rootkits ». Ces outils insidieux tentent de charger des programmes malveillants le plus tôt possible, si bien qu'ils parviennent à rester inaperçus grâce aux privilèges élevés dont ils bénéficient dans le système. La technologie anti-rootkit de Kaspersky Lab est capable de détecter et de supprimer les programmes malveillants les mieux cachés. Elle fonctionne aussi bien au niveau de la mémoire que du système de fichiers et nécessite l'accès à la mémoire RAM et aux processus de la machine invitée.

Kaspersky Security for Virtualization | Light Agent est en mesure de proposer cette technologie, car le produit bénéficie d'un accès complet aux ressources de la machine invitée.

Kaspersky Security for Virtualization | Agentless ne peut accéder qu'au système de fichiers sans bénéficier de la fonction complète anti-rootkit.

ATTAQUES RÉSEAU

Certaines menaces exploitent les fonctions du système de mise en réseau et permettent aux programmes malveillants d'obtenir des informations cruciales sur le réseau, d'accéder aux ressources système cibles ou d'entraver son bon fonctionnement. Il peut s'agir, par exemple, de balayage des ports, d'attaques par déni de service, d'attaques par sous-alimentation de la mémoire tampon ou toute autre action malveillante. Ces attaques nécessitent un arsenal de contre-mesures comme celles de la technologie Network Attack Blocker de Kaspersky. Cette technologie bloque les attaques réseau entrantes à l'aide du système de détection des intrusions (IDS) grâce à des algorithmes heuristiques permettant de distinguer les schémas d'attaque les plus complexes.

Les solutions **Kaspersky Security for Virtualization | Agentless** et **Kaspersky Security for Virtualization | Light Agent** proposent toutes les deux ces technologies réseau dans leur arsenal de défense.

SITES WEB MALVEILLANTS

Un site Web infecté ou malveillant figure aujourd'hui parmi les sources d'infection les plus courantes. Même si cette situation concerne rarement les serveurs virtuels, elle peut représenter un risque sérieux pour les infrastructures de postes de travail virtuels si les utilisateurs disposent d'un accès complet à Internet. C'est dans ce contexte que les technologies Web de Kaspersky Lab entrent en jeu. La fonctionnalité antiphishing empêche les utilisateurs d'accéder aux sites Web signalés comme dangereux en exploitant les informations obtenues à partir du réseau **Kaspersky Security Network** et mises à jour régulièrement par des millions de participants volontaires dans le monde. Les sites de phishing jusqu'à présent non répertoriés sont aussi bloqués grâce à un moteur heuristique qui analyse le texte source de la page chargée pour y détecter des traces de code malveillant. La technologie de **contrôle du Web** offre l'avantage de restreindre l'accès aux sites Web non liés aux activités professionnelles, comme les sites de jeux ou les réseaux sociaux, tout en empêchant les utilisateurs de perdre leur temps dans des activités non professionnelles.

Kaspersky Security for Virtualization | Agentless ne comporte pas ces fonctions hébergées sur l'hôte, contrairement à **Kaspersky Security for Virtualization | Light Agent**, qui s'avère une solution plus adaptée aux infrastructures de postes de travail virtuels disposant d'un accès Internet.

ATTAQUES PÉRIPHÉRIQUES

Habituellement, le stockage externe représente le moyen le plus efficace pour introduire un virus dans un réseau informatique. Si les infections issues des réseaux représentent désormais la menace la plus sérieuse au regard des statistiques, le stockage externe constitue encore un danger non négligeable, notamment dans le cadre d'une attaque ciblée soigneusement planifiée. Il convient de mentionner que les périphériques non liés au stockage et non contrôlés peuvent également représenter un certain risque ; parmi les cas connus, citons, par exemple, l'infection des micrologiciels d'imprimante. L'exploitation des disques de stockage externes fait aussi partie des méthodes de vol de données confidentielles les plus courantes.

S'il est généralement difficile pour une personne non autorisée d'accéder aux machines physiques hébergeant l'infrastructure virtuelle, cette possibilité n'est toutefois pas à exclure totalement. Dans certaines situations professionnelles, ce risque est même jugé trop élevé. Par ailleurs, dans le cas d'une infrastructure de postes de travail virtuels, même le client léger le plus simple peut posséder des ports USB.

Le contrôle des périphériques s'avère donc une précaution judicieuse et sa prise en charge est assurée en toute simplicité par la technologie **de contrôle des périphériques de Kaspersky Lab**. Cette dernière permet la prévention ou la restriction de l'utilisation de types de bus ou de périphérique spécifiques. Il est bien sûr possible de configurer des exceptions afin de pouvoir continuer à utiliser les périphériques essentiels aux activités professionnelles.

Comme les autres technologies de contrôle, le contrôle des périphériques est proposé dans **Kaspersky Security for Virtualization | Light Agent**, mais pas dans **Kaspersky Security for Virtualization | Agentless.**

FUITES DE DONNÉES

La divulgation de secrets professionnels depuis un réseau informatique peut avoir des effets dévastateurs sur une entreprise, notamment sur sa réputation, ainsi que des conséquences désastreuses à long terme. Il peut donc s'avérer indispensable de restreindre les modes d'échange des informations. Les solutions de **contrôle des applications** et **des périphériques** de Kaspersky Lab sont utiles dans ce genre de situation. Le contrôle des applications peut bloquer l'exécution d'applications dangereuses, telles que les messageries instantanées ou les applications clientes P2P et d'hébergement de fichiers. Le contrôle des périphériques, quant à lui, limite l'utilisation du stockage externe, susceptible d'être exploité pour diffuser des données sensibles.

Là encore, ces deux technologies sont incluses dans **Kaspersky Security for Virtualization | Light Agent**, mais pas dans **Kaspersky Security for Virtualization | Agentless**.

SANS AGENT OU AVEC AGENT LÉGER : QUELLE STRATÉGIE CHOISIR ?

Pour certains lecteurs, la réponse ne fait aucun doute : **Kaspersky Security for Virtualization | Light Agent** propose des fonctions avancées qui ne figurent pas dans **Kaspersky Security for Virtualization | Agentless**. De toute évidence, la solution de l'agent léger représente le meilleur choix. Mais ne tirons pas de conclusions hâtives : la question n'est pas aussi simple qu'elle n'y paraît.

Il convient en effet de prendre en compte la question de la protection immédiate proposée par **Kaspersky Security for Virtualization | Agentless**. Les machines virtuelles sont protégées dès leur démarrage, ce qui représente un atout majeur si votre réseau virtuel est déjà infecté. (Par ailleurs, votre machine virtuelle ne peut pas être générée depuis une image contenant l'application **Light Agent**.)

Là encore, dans certains cas, il est possible que les performances de **Kaspersky Security for Virtualization | Light Agent** soient inférieures à celles de **Kaspersky Security for Virtualization | Agentless**. Pour choisir l'option de sécurité qui convient le mieux à votre installation virtuelle et gérer au mieux votre projet de virtualisation, vous devrez évaluer les risques potentiels, la valeur des données à protéger et les différentes couches de protection nécessaires.

Veuillez noter que toute combinaison d'une protection sans agent pour VMware et d'une sécurité basée sur un agent léger pour l'une des trois plates-formes ou l'ensemble d'entre elles est prise en charge par une seule licence **Kaspersky Security for Virtualization**. Que vous utilisiez Citrix, VMware ou Microsoft, ces solutions sont toutes placées sous votre contrôle à partir de l'interface conviviale centralisée de **Kaspersky Security Center**.

KASPERSKY lab