KASPERSKY lab

AGENT LÉGER OU SANS AGENT ?

Les fonctionnalités de Kaspersky Security for Virtualization

www.kaspersky.fr

Avec la généralisation grandissante de la virtualisation, le besoin de solutions de sécurité est une évidence. Bien qu'ils soient aussi vulnérables aux cyberattaques que tout autre système physique, les environnements virtuels présentent des spécificités dont il convient de tenir compte lors de l'évaluation de plusieurs solutions de sécurité.

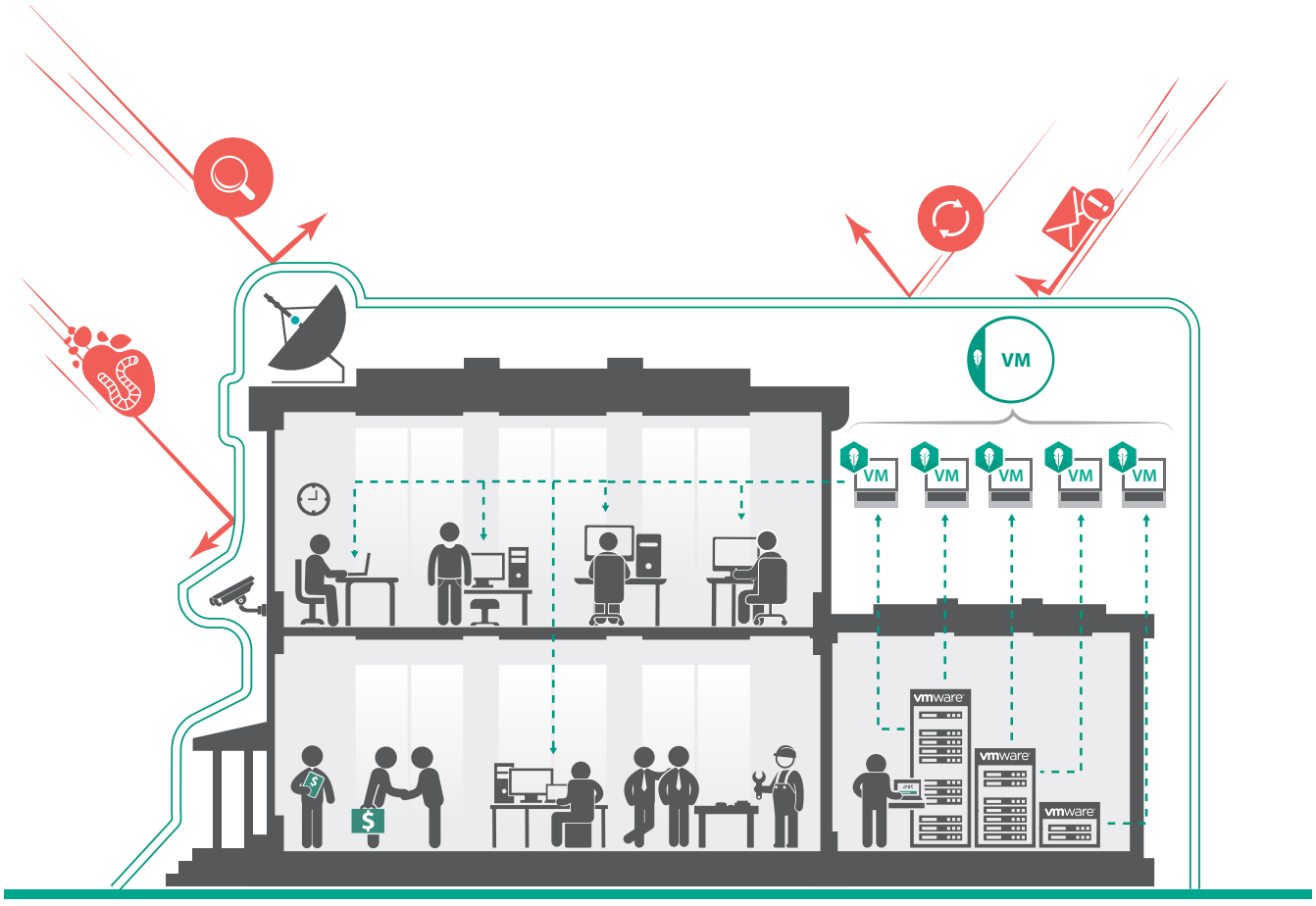
Les entreprises peuvent utiliser la même solution de sécurité pour protéger leurs machines physiques et virtuelles. Si elles offrent un bon niveau de protection, les solutions standard qui ne sont pas conçues spécifiquement pour des environnements virtuels peuvent néanmoins présenter les problèmes suivants :

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 chaque machine virtuelle. 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. **Failles instantanées (instant-on gap).** Il n'est pas possible de mettre à jour les bases de données de signature sur des machines virtuelles inactives. La machine virtuelle est donc vulnérable face aux attaques, de son démarrage jusqu'à la fin du processus de mise à jour.
4. **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 de virtualisation vSphere. Cette couche crée un espace de sécurité intégré pour les solutions tierces bénéficiant d'une intégration native avec des API VMware comme vShield Endpoint et NSX Guest Introspection, 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. Il ne suffit que d'une seule appliance

virtuelle de sécurité par hôte, 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. Cette approche offre aux grandes entreprises le bénéfice d'une intégration native et fluide avec l'écosystème VMware.

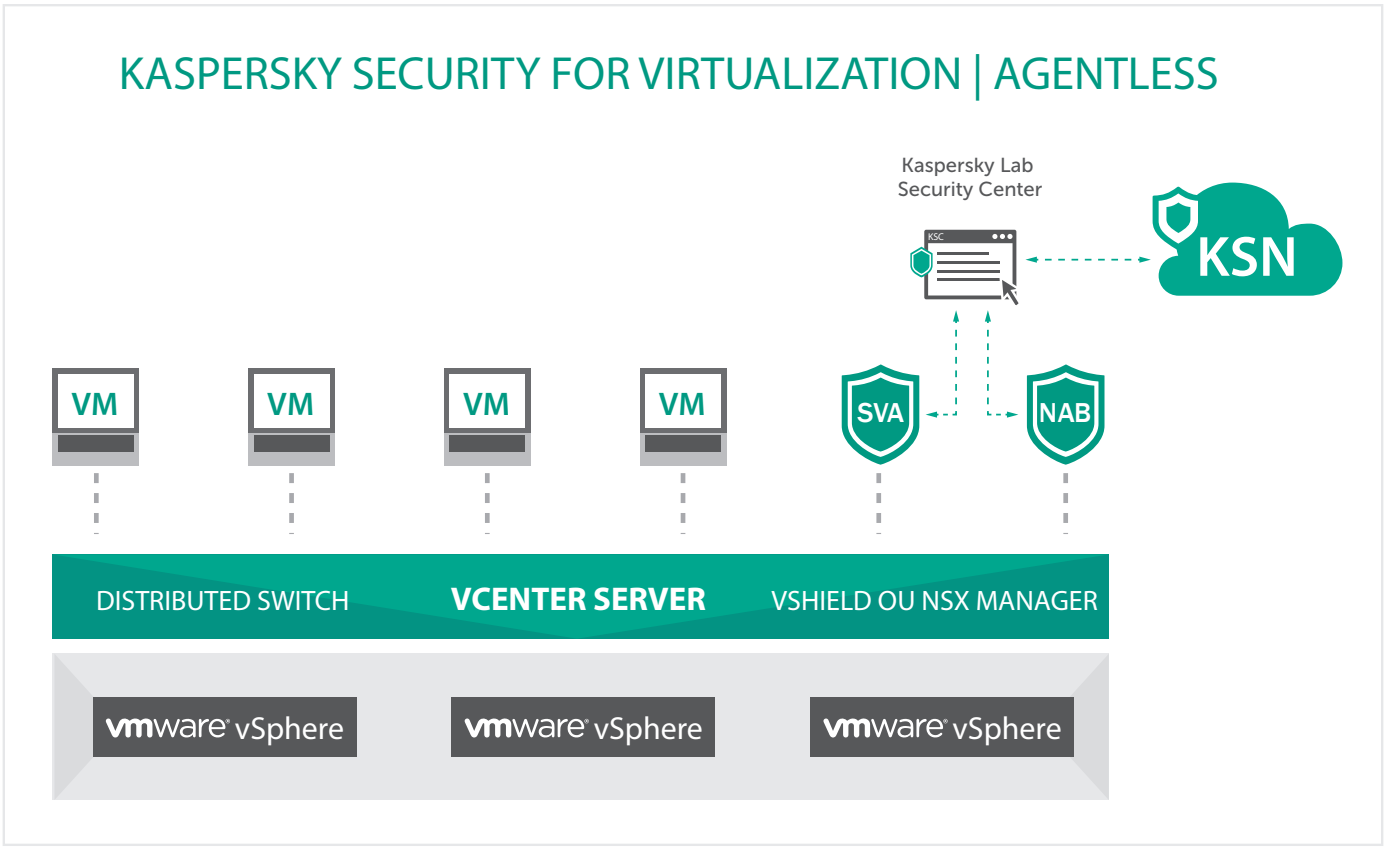
Autre approche : une solution indépendante de l'API, ou plutôt, une solution indépendante de la plate-forme de virtualisation, qui utilise un agent léger optimisé pour fonctionner au sein du système d'exploitation de chaque machine virtuelle protégée. Dans la mesure où le moteur d'analyse des fichiers et les bases de données sont centralisés sur l'appliance virtuelle de sécurité, cette technologie « agent léger » nécessite considérablement moins de ressources que la solution complète basée sur un agent. Il s'agit d'une solution intermédiaire entre la protection « sans agent » et la solution complète basée sur un agent en termes de consommation des ressources mais elle n'est pas liée à ou limitée par les technologies VMware et elle peut aussi être utilisée sur les plates-formes les plus répandues, dont Microsoft Hyper-V, Citrix XenServer et KVM.



KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless est spécifiquement conçu pour exploiter tous les avantages de la technologie vShield Endpoint. Reposant sur la technologie primée du moteur de protection contre les programmes malveillants de Kaspersky Lab, l'appliance virtuelle de sécurité conçue pour un déploiement prêt à l'emploi offre des performances et des taux de détection de premier ordre. La prise en charge du service Kaspersky Security Network (KSN) basé dans le Cloud permet les temps de réaction les plus rapides et est capable d'identifier de nouveaux programmes malveillants dans un délai de 0,02 seconde. Kaspersky Security for Virtualization peut ainsi protéger votre environnement virtuel contre les menaces de type « zero-day ».

Les environnements dotés de VMware NSX bénéficient d'une intégration entre Kaspersky Security for Virtualization | Agentless et la technologie NSX Guest Introspection native de VMware, permettant à votre infrastructure de s'adapter sans limite pendant que votre solution de sécurité suit les changements de topologie et d'infrastructure, de façon fluide.
Pour une protection avancée du réseau, il est également possible de faire appel à une deuxième appliance afin d'exploiter la fonctionnalité de prévention des intrusions de Kaspersky Lab en intégration étroite avec le composant de sécurité et réseau vCloud de VMware.

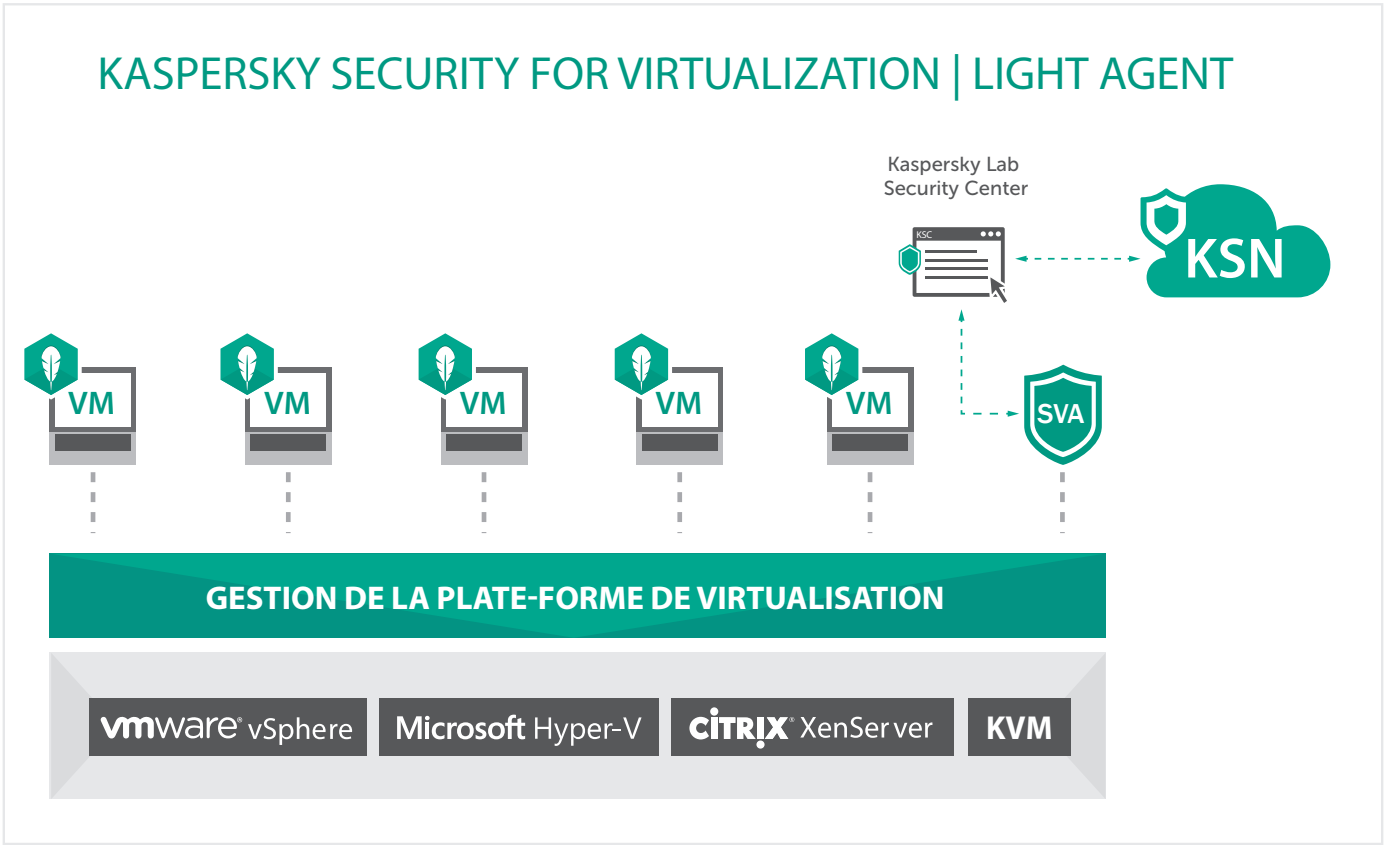


Une approche « sans agent » présente des inconvénients. Tout d'abord, VMware vSphere est la seule plate-forme de virtualisation disposant d'un niveau intermédiaire de sécurité, vShield Endpoint. Pour les autres plates-formes de virtualisation, la solution de sécurité doit installer un agent au sein du système d'exploitation invité de chaque machine virtuelle, afin d'effectuer des tâches d'analyse des fichiers au niveau de la machine. Puis, en raison de la conception de VMware, les technologies natives comme vShield Endpoint et NSX Guest Introspection ne fournissent pas d'accès aux processus internes, applications ou trafic Web de la machine virtuelle ou aux appareils virtualisés. La protection de l'infrastructure est limitée à l'analyse des fichiers, ce qui réduit fortement la capacité de la solution à offrir au niveau de chaque machine virtuelle une protection renforcée contre des programmes malveillants élaborés.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Une protection avec « agent léger » contourne ces limites. Dans la mesure où le moteur d'analyse des fichiers et les bases de données sont centralisés sur l'appliance virtuelle de sécurité, cette dernière exige considérablement moins de ressources que les solutions complètes basées sur un agent. L'agent léger sur chaque machine virtuelle fournit l'accès à la mémoire des machines individuelles, aux applications et aux processus internes, ainsi qu'au trafic Web et aux appareils virtualisés. Cet accès permet le déploiement de techniques de sécurité avancées au niveau de la machine, tout en préservant l'efficacité et la performance globales de la plate-forme de virtualisation.

Kaspersky Security for Virtualization | Light Agent est spécialement conçu pour protéger les environnements virtuels et prend en charge les plates-formes les plus répandues : Citrix XenServer, Microsoft Hyper-V, VMware et plus récemment KVM.



Dans les environnements de serveurs virtualisés, les utilisateurs de Kaspersky Security for Virtualization | Light Agent bénéficient de technologies précieuses comme HIPS (Host-Based Intrusion Prevention System - Système de prévention des intrusions hébergé sur l'hôte) et d'un pare-feu propriétaire, protégeant contre les attaques réseau. Pour les environnements VDI, la sécurité est plus poussée avec des fonctionnalités étendues de protection du réseau et un ensemble complet de contrôles des terminaux, vous permettant non seulement de protéger vos systèmes des programmes malveillants, mais aussi de limiter l'utilisation d'applications, d'appareils ou de ressources Web non fiables. L'architecture de la solution réduit significativement la surface d'attaque, économisant ainsi de précieuses ressources informatiques. La technologie de protection automatique contre les Exploits vient compléter un puissant périmètre défensif multi-niveaux, capable d'éliminer les programmes malveillants sophistiqués ainsi que les menaces « zero-day ».

Une protection avec « agent léger » signifie que vous pouvez sécuriser votre environnement virtuel (y compris les serveurs et l'infrastructure de postes de travail virtuels), avec une incidence minimale sur les performances de l'hyperviseur. Vous êtes ainsi en mesure de protéger vos systèmes et données d'entreprise sensibles, tout en préservant la densité des machines et la qualité de l'expérience utilisateur.

LES TECHNOLOGIES DE PROTECTION DE KASPERSKY LAB OU LES MENACES QUI GUETTENT VOTRE INFRASTRUCTURE VIRTUELLE

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 une solution de sécurité efficace dotée de la protection nécessaire pour lutter contre les menaces sophistiquées. 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 une protection contre les programmes malveillants pour traiter ces menaces de base. Notre puissant moteur de protection contre les programmes malveillants est au cœur des solutions sans agent et avec agent léger de Kaspersky Security for Virtualization, même s'ils accèdent 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 empêcher les programmes malveillants, il convient de n'autoriser que l'exécution de logiciels fiables. Kaspersky Security for Virtualization | Light Agent permet le contrôle des terminaux, y compris le contrôle des applications, sur chaque machine virtuelle.

Programmes malveillants sans corps

Certains programmes malveillants n'ont pas de « corps », ils sont donc 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 peut rarement être détecté par les solutions traditionnelles de protection contre les programmes malveillants. Il convient, dans ce cas, d'utiliser des techniques de protection avancées, capables de surveiller les processus en mémoire et de bloquer immédiatement les programmes dont l'activité semble suspecte ou dangereuse.

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.
- Behavioral Stream Signatures, qui identifie les schémas comportementaux caractéristiques de l'activité des programmes malveillants.
- Privilege Control, 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.

Exploitation de failles

L'exploitation des failles identifiées dans les composants du système et les applications les plus connues est une stratégie d'attaque extrêmement efficace. S'il est possible de contrer ces intrusions à l'aide des technologies ci-dessus, 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'exploiter leurs vulnérabilités cibles. Pour surmonter rapidement les dangers posés par les vulnérabilités non corrigées, Kaspersky Security for Virtualization | Light Agent offre une technologie de protection automatique contre les Exploits. L'AEP surveille tout particulièrement les applications les plus souvent prises pour cible dans les environnements critiques comme les environnements VDI , parmi lesquelles Adobe Reader, Internet Explorer, Microsoft Office, Java et bien d'autres, pour offrir un niveau supplémentaire de surveillance de la sécurité et de protection contre les menaces inconnues.

L'efficacité de cette technologie a été confirmée par des tests indépendants réalisés par l'institut MRG Effitas, dont les résultats ont révélé que la technologie de prévention automatique des failles 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 (voir la « Prévention des vulnérabilités d'entreprise en live », MRG Effitas, mars 2015 pour en savoir plus). Les failles « zero-day » inconnues ne font pas exception à la règle et sont également bloquées par cette technologie performante.

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 démarrer ou d'exécuter les programmes malveillants le plus tôt possible, si bien qu'ils parviennent à ne pas être détectés grâce aux privilèges élevés dont ils bénéficient dans le système d'exploitation invité.

Fonctionnant aussi bien au niveau de la mémoire que du système de fichiers, Kaspersky Security for Virtualization | Light Agent utilise la technologie antirootkit de Kaspersky Lab pour détecter et supprimer les programmes malveillants les mieux cachés.

Attaques réseau

Les cybermenaces basées sur le réseau peuvent permettre au pirate informatique d'obtenir des informations cruciales sur le réseau, d'accéder aux ressources systèmes cibles, d'entraver des processus stratégiques et de perturber son bon fonctionnement. Ces menaces comprennent des actions malveillantes comme le balayage des ports, les attaques par déni de service, les attaques par sous-alimentation de la mémoire tampon. Nos solutions « sans agent » et « agent léger » comportent des technologies intégrées de protection réseau. Kaspersky Security for Virtualization | Light Agent étend les fonctionnalités de protection du réseau avec un système de prévention des intrusions sur l'hôte (HIPS) intégré et des technologies propriétaires supplémentaires pour lutter contre les attaques réseau externes et internes, y compris les menaces pouvant être dissimulées dans le trafic virtuel non transparent.

Kaspersky Security for Virtualization | Agentless traite ce problème, en exploitant l'intégration à VMware afin de fournir une prévention des intrusions, une appliance virtuelle dédiée conçue pour surveiller le trafic réseau à la recherche des activités emblématiques des attaques.

Sites Web malveillants

Les sites Internet infectés ou malveillants figurent 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 virtuelles, ce dont les utilisateurs en entreprise ne sont pas toujours conscients. C'est dans ce contexte que les technologies de protection Internet de Kaspersky Lab entrent en jeu.

La fonctionnalité antiphishing empêche les utilisateurs d'accéder aux sites Internet signalés comme dangereux en exploitant les informations obtenues à partir du réseau Kaspersky Security Network (KSN) 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. Le contrôle du Web vous permet de gérer l'utilisation d'Internet. Vous pouvez ainsi bloquer l'accès aux réseaux sociaux, à la musique, aux vidéos, aux messageries Web non professionnelles et à tout site Web présentant du contenu inapproprié ou allant à l'encontre de la politique de votre entreprise. Vous pouvez déployer des politiques différentes afin de refléter différentes responsabilités et choisir entre appliquer un blocage complet ou bloquer simplement l'accès durant des périodes spécifiques.

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 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. L'exploitation des disques de stockage externes fait partie des méthodes de vol de données confidentielles les plus courantes. S'il est relativement difficile pour une personne non autorisée d'accéder aux machines physiques hébergeant l'infrastructure virtuelle, cette possibilité n'est toutefois pas à exclure totalement.

Par conséquent, il est important de se soucier de la connexion du matériel à votre environnement virtualisé. Par exemple, il est recommandé d'utiliser des clients légers pour les déploiements sur les PC virtualisés, puisque même le client léger le plus simple possède des ports USB. Le contrôle des périphériques peut être un cauchemar, ou il peut être effectué en toute simplicité grâce à la technologie de contrôle des appareils de Kaspersky Lab. Cette technologie vous permet de spécifier quels dispositifs amovibles sont autorisés à accéder aux machines virtuelles individuelles. Les politiques de contrôle peuvent donc être appliquées très facilement à une large gamme d'appareils, notamment les lecteurs amovibles, imprimantes et connexions réseau non professionnelles.

Fuites de données

La divulgation de secrets depuis un réseau informatique professionnel peut non seulement avoir des effets dévastateurs sur les systèmes ou processus métier essentiels, mais aussi sur toute l'entreprise, notamment sur sa réputation, ainsi que des conséquences désastreuses à long terme. Restreindre les modes d'échange des informations peut être une bonne solution pour protéger votre entreprise.

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 voler des données sensibles. Ces deux technologies sont incluses dans Kaspersky Security for Virtualization | Light Agent.

Sans agent ou avec agent léger : quelle stratégie choisir ?

La réponse dépend de la ou des plates-formes de virtualisation que vous utilisez et des déploiements spécifiques. Quel que soit l'hyperviseur utilisé pour concevoir votre environnement virtualisé (VMware vSphere, Citrix XenServer, Microsoft Hyper-V ou KVM), vous pouvez protéger vos serveurs virtuels essentiels et votre infrastructure de bureaux virtuels avec Kaspersky Security for Virtualization | Light Agent. Mais vous pouvez aussi envisager Kaspersky Security for Virtualization | Agentless pour les serveurs VMware non essentiels qui ne nécessitent pas une sécurité multi-niveaux aussi efficace.

Heureusement, la politique de licence de Kaspersky Security for Virtualization vous permet de déployer l'approche la mieux appropriée à chaque partie de votre environnement virtualisé (« sans agent », « agent léger » ou les deux) à l'aide d'une seule licence.

Quelle que soit la combinaison de plates-formes de virtualisation Citrix XenServer, VMware vSphere, KVM ou Microsoft Hyper-V, et quelle que soit votre approche, vous pouvez gérer la sécurité de toutes vos machines, virtuelles et physiques, ainsi que de vos appareils mobiles, depuis une seule console unifiée : Kaspersky Security Center. De plus, l'utilisation de notre service de sécurité basé dans le Cloud (Kaspersky Security Network) permet une détection instantanée des menaces sophistiquées.