KASPERSKY lab

RECHERCHE MONDIALE SUR LA SÉCURITÉ INFORMATIQUE

LA VIRTUALISATION EN TOUTE SÉCURITÉ : À LA RECHERCHE DU JUSTE ÉQUILIBRE

Conjuguer protection et performance au sein de votre environnement virtuel

#EnterpriseSec
kaspersky.com/enterprise

TABLE DES MATIÈRES

INTRODUCTION

LA VIRTUALISATION A TRANSFORMÉ L'ENVIRONNEMENT INFORMATIQUE DES ENTREPRISES

Jamais les organisations du monde entier n'ont dû faire face à un niveau de cyber-menaces aussi élevé qu'aujourd'hui. Il est donc indispensable que l'infrastructure informatique, aussi bien physique que virtuelle, soit sécurisée intégralement et efficacement.

L'ajout de fonctionnalités de sécurité au sein d'un système informatique implique, de fait, une augmentation de la consommation des ressources. L'objectif consiste donc à veiller systématiquement à optimiser la protection sans trop nuire aux performances en trouvant le juste équilibre entre sécurité et efficacité des systèmes.

Il s'agit d'une problématique particulièrement délicate pour toute infrastructure virtuelle. L'efficacité des performances, l'optimisation des activités et la réduction des coûts qui en découle représentent les avantages les plus importants que la virtualisation peut offrir aux entreprises. Or, l'installation de solutions de sécurité consommant d'importantes ressources sur des systèmes virtuels risque d'atténuer ces avantages et de remettre en cause l'intérêt premier d'investir dans une solution de virtualisation.

Il n'est pas si évident de sélectionner la solution de sécurité qui convient le mieux à un environnement virtuel spécifique.
Cet article vous aide à identifier l'approche la mieux adaptée à votre environnement virtuel : une approche reposant sur la recherche du meilleur équilibre entre sécurité et performances. Ce « juste équilibre » étant légèrement différent d'une organisation à une autre, il est impossible de proposer une seule et unique réponse. Néanmoins, tout repose avant tout sur la mise en place d'un agent de sécurité au niveau des terminaux virtuels et sur le choix de son format. La difficulté ? Mettre en œuvre des fonctions de sécurité au niveau des terminaux sans pour autant occuper une trop grande quantité d'espace à cet effet.

Nous présenterons trois approches en matière de sécurité des terminaux virtuels, ainsi que les critères permettant d'obtenir le meilleur retour sur investissement. Nous expliquerons également comment bénéficier de performances optimales et trouver le juste équilibre en matière de sécurité au niveau de vos environnements virtuels, physiques et mobiles.

Les trois approches sont les suivantes :
- Protection basée sur un agent
- Protection sans agent
- Protection avec agent léger

Il est indispensable de comprendre parfaitement ces différentes approches ainsi que leurs forces et leurs faiblesses afin de trouver l'équilibre qui vous convient le mieux.

VIRTUALISATION

UNE ÉTUDE MENÉE RÉCEMMENT PAR GARTNER RÉVÈLE QU'UN PEU PLUS DE 60 % DES PERSONNES INTERROGÉES DÉCLARENT QUE LEUR ENTREPRISE PROCÈDE DÉJÀ À LA VIRTUALISATION DES POSTES DE TRAVAIL SOUS UNE FORME OU UNE AUTRE.[1]

D'APRÈS LES PRÉVISIONS DE GARTNER, LE MARCHÉ DES POSTES DE TRAVAIL VIRTUELS HÉBERGÉS DEVRAIT ENREGISTRER UNE CROISSANCE TOTALE DE 13,14 % À L'ÉCHELLE MONDIALE AU COURS DE L'ANNÉE 2014, PUIS PROGRESSER RÉGULIÈREMENT ET ATTEINDRE 7,38 % 2017.[2]

La virtualisation des serveurs et des postes de travail peut présenter d'énormes avantages commerciaux.

En voici quelques exemples significatifs :

- Maîtrise des coûts : la virtualisation permet de réduire les ressources et les dépenses matérielles, l'encombrement au sol, la consommation d'énergie, les besoins en termes d'administration, etc.
- Vitesse : la virtualisation accélère les traitements informatiques en renforçant les capacités à la demande. Cette agilité débouche sur une plus grande compétitivité à tous les niveaux de l'entreprise.
- Stabilité : les systèmes simplifiés, standardisés et redondants sont la garantie d'une plus grande résistance, d'une meilleure disponibilité et d'une plus grande productivité des employés, partout et à tout moment.
- Administration centralisée : les systèmes virtuels peuvent être créés instantanément, puis gérés et configurés de manière centralisée, ce qui permet de réduire les coûts d'administration et de support.

En résumé, les entreprises font le choix de la virtualisation, car celle-ci permet d'optimiser l'efficacité informatique et, de ce fait, de réduire les coûts.

1 Tendances du marché : virtualisation des postes de travail, 2013, 10 octobre 2013 – Gartner, Inc.
2 Prévisions : marchés des logiciels d'entreprise, 2010 – 2017, informations du 4e trimestre 2013 – Gartner, Inc.

SÉCURITÉ VIRTUELLE : LES RISQUES

DÉBUT 2011, KASPERSKY LAB ASSURAIT LE SUIVI DE 35 MILLIONS DE MENACES AU SEIN DE SA BASE DE DONNÉES PRINCIPALE. UN AN PLUS TARD, CE CHIFFRE A PRATIQUEMENT DOUBLÉ POUR ATTEINDRE 67 MILLIONS. DÉSORMAIS, KASPERSKY LAB DÉTECTE EN MOYENNE 315 000 NOUVELLES MENACES CHAQUE JOUR.

LES MACHINES VIRTUELLES (VM) SONT-ELLES INTRINSÈQUEMENT PLUS SÉCURISÉES QUE LES MACHINES PHYSIQUES ?

La réponse est non. S'il existe quelques vecteurs d'attaque auxquels les machines virtuelles sont moins exposées (les menaces de ransomeware, par exemple), elles sont tout aussi vulnérables aux principales formes de programmes malveillants, comme les pièces jointes des e-mails, les téléchargements intempestifs, les chevaux de Troie de type botnet, les vers infectant les réseaux, voire les attaques par phishing ciblé.

Ces menaces persistent lorsque le système virtuel est actif et en cours d'utilisation.

Selon le National Institute of Standards and Technology (NIST) :

« La virtualisation ajoute des couches de technologie, ce qui peut alourdir la gestion de la sécurité en impliquant des contrôles de sécurité supplémentaires. La combinaison de plusieurs systèmes au sein d'un même ordinateur physique peut avoir des conséquences plus ravageuses en cas de brèche dans la sécurité. De plus, les systèmes de virtualisation qui s'appuient sur une infrastructure de ressources partagées représentent un vecteur d'attaque des plus dangereux dans la mesure où une seule machine virtuelle contaminée est susceptible de compromettre l'ensemble de l'infrastructure virtuelle. »[3]

L'environnement virtuel comporte d'autres risques :

- Infection au niveau du réseau : les programmes malveillants, neutralisés sur une machine virtuelle non persistante lorsque celle-ci est déconnectée, auront sans doute déjà infecté d'autres machines sur le réseau virtuel. Compte tenu des vitesses que ces réseaux peuvent atteindre, l'infection peut se propager comme un feu de brousse et infecter les nouvelles machines au fur et à mesure.
- Infection au niveau du stockage : les programmes malveillants peuvent également se répandre en infectant les magasins de données auxquels accèdent les machines virtuelles.
- Une machine virtuelle peut être utilisée pour « épier » le trafic d'une autre machine.
- Les auteurs de programmes malveillants élargissent également leur stratégie d'attaque à l'aide de code ciblant aussi bien les machines virtuelles que les machines physiques.

LES MENACES QUE REPRÉSENTENT LES PROGRAMMES MALVEILLANTS PROGRESSENT À UN RYTHME ALARMANT

Début 2011, Kaspersky Lab assurait le suivi de 35 millions de menaces au sein de sa base de données principale. Un an plus tard, ce chiffre a pratiquement doublé pour atteindre 67 millions. Désormais, Kaspersky Lab détecte en moyenne 315 000 nouvelles menaces chaque jour.

Qu'il s'agisse de frappes éclairs sur la chaîne d'approvisionnement ou d'« attaques de type watering-hole » associant les attaques de « phishing ciblé » et les téléchargements intempestifs, les armes de la cyber-guerre utilisées contre les organisations sont de plus en plus sophistiquées. Personne n'est aujourd'hui à l'abri.

« Toute entreprise peut un jour ou l'autre en être victime. Elles possèdent toutes des données susceptibles d'intéresser les cyber-criminels ou de servir de passerelles vers d'autres entreprises. **David Emm de l'équipe Kaspersky GReAT (Global Research and Analysis Team)**[4]

En un mot, les entreprises ont plus que jamais besoin de protéger leurs systèmes informatiques, tant sur le plan physique que virtuel.

Les entreprises, et notamment les multinationales, qui adoptent la technologie de virtualisation sont aujourd'hui des proies intéressantes aux yeux des cyber-criminels, qui ne cessent d'optimiser leurs performances et redoublent d'effort pour infiltrer, infecter et manipuler les systèmes virtuels.

3 Guide to Security for Full Virtualization Technologies, National Institute of Standards & Technology, 2011
4 Bulletin Kaspersky Lab sur la sécurité 2013

SÉCURITÉ VIRTUELLE : L'ÉQUILIBRE PARFAIT

Les organisations investissent dans des solutions de virtualisation afin de gagner en efficacité et réduire leurs coûts. Dans cette optique, il est nécessaire de préserver l'optimisation des performances. Or, les capacités des systèmes sont phagocytées, entre autres, par les logiciels de sécurité.

Il arrive parfois en effet que certains antivirus alourdissent l'infrastructure virtuelle, affaiblissant ainsi les ratios de consolidation et compromettant le retour sur investissement. Un livre blanc consacré à une étude comparative en matière de sécurité souligne que certaines configurations antivirus peuvent réduire jusqu'à 40 % les capacités de l'hôte hébergeant les postes virtuels.[5]

Mais les systèmes virtuels sont malgré tout vulnérables aux cyber-menaces et doivent être protégés. Quels que soient les coûts de mise en œuvre d'une solution de sécurité, ils seront sans aucun doute largement inférieurs aux coûts liés à l'infraction dont sera victime votre système et qui pourrait suffire, rien qu'en termes d'atteinte à l'image de marque, à mettre en péril l'ensemble de votre organisation.

Le mythe selon lequel les environnements virtuels sont, par nature, sécurisés et qu'ils ne nécessitent aucune protection appartient désormais au passé. La faute, dans une large mesure, aux cyber-criminels du monde entier, dont les efforts acharnés ont permis d'identifier depuis longtemps les nouvelles opportunités offertes par les systèmes virtuels et de les exploiter aujourd'hui.
(Par exemple, Morcut, appelé également Crisis, le premier cheval de Troie à cibler les machines virtuelles et dont l'identification remonte à 2012).

Il reste cependant difficile de sauter le pas et d'investir dans une solution de sécurité visant à offrir aux systèmes virtuels le même niveau de protection que les systèmes physiques.

Les entreprises sont en effet aujourd'hui « promptes à la virtualisation, mais peu réactives pour la mise en place d'une solution de sécurité ». Pourquoi un tel paradoxe ? Gartner est parvenu à résumer très simplement le fond du problème :

« La sécurisation de la plate-forme [virtuelle] a un prix, que ce soit au niveau des licences du logiciel de sécurité ou de l'impact potentiel sur les performances. Les produits d'analyse des programmes malveillants risquent d'entraver sensiblement les capacités d'une plate-forme, notamment s'ils ne sont pas configurés de façon optimale pour l'environnement ». [6]

L'investissement dans une solution de virtualisation se justifie avant tout par les gains de performances et la réduction des coûts dont il est possible de bénéficier. Or, si les capacités de la plate-forme sont affectées à cause d'un logiciel de sécurité conçu et configuré de façon inappropriée, cette justification ne tient plus.

Jusqu'à présent, les options disponibles pour protéger les machines virtuelles contre les programmes malveillants reposaient toutes sur un compromis peu satisfaisant entre protection, performances et gestion.

Que peut donc faire un responsable informatique pour préserver un environnement virtuel efficace et correctement protégé tout en bénéficiant des avantages métiers de la virtualisation ? Où se situe l'équilibre et comment peut-on y parvenir ?

La réponse est à chercher du côté de la conception du système de sécurité. Il convient de vérifier si l'architecture a été développée ou non pour répondre aux contraintes spécifiques des environnements virtuels et de s'assurer notamment de la présence et du bon fonctionnement d'un agent de sécurité au niveau du terminal virtuel.

Passons maintenant en revue les trois approches : la sécurité avec agent, sans agent et avec un agent léger.

5 Phase 5 – Antivirus et meilleures pratiques dans les infrastructure de postes de travail virtuels V1, janvier 2013, Projet Virtual Reality Check (VRC)
6 Connaître les implications de sécurité liées à l'adoption des postes de travail virtuels hébergés, 8 avril 2013 – Gartner, Inc.

PROTECTION BASÉE SUR UN AGENT

Parmi les différentes approches, il est possible d'utiliser une solution de sécurité classique basée sur un agent. Une solution de cette nature implique le chargement d'une copie complète du logiciel antivirus sur chaque machine virtuelle, exactement de la même façon qu'avec la plupart des solutions de sécurité propres aux terminaux physiques.

Si cette approche permet un niveau de sécurité relativement élevé, les coûts correspondants sont généralement très élevés en termes de ressources et de niveaux de performance lors du déploiement d'un logiciel conçu pour des environnements physiques.

AVANTAGES

- L'extension à l'environnement virtuel d'un système de sécurité physique offre le double avantage de pouvoir bénéficier d'un fonctionnement familier et de ne pas avoir à initier un nouveau processus d'approvisionnement.
- Il est possible de réaliser des économies d'échelle et des gains d'efficacité en utilisant un seul système de sécurité sur les environnements physiques et virtuels.
- Il se peut que les organisations possédant peu de machines virtuelles et n'ayant pas l'intention d'en acheter d'autres ne voient pas l'intérêt d'investir financièrement dans un logiciel de sécurité spécialement conçu pour la virtualisation.

CONTRAINTES

Affaiblissement des performances

La base de données de signatures et le logiciel antivirus étant installés sur chaque machine virtuelle, les performances des systèmes virtuels peuvent être sérieusement compromises. La duplication des bases de données de signatures et l'analyse redondante des fichiers consomment inutilement de précieuses ressources système. Par ailleurs, ce type de redondance met à mal la disponibilité de la mémoire, du stockage et du micro-processeur, ce qui a pour effet d'augmenter la consommation des ressources et de réduire les ratios de consolidation.

Conflit d'accès aux ressources partagées et « blitz antivirus » (« AV-Storm »)

Étant donné que chacun des agents installés sur les terminaux virtuels se charge de toutes les tâches de sécurité d'une manière indépendante, le conflit d'accès aux ressources partagées devient problématique.

Parmi les symptômes figurent notamment les points suivants :

- « **Blitz antivirus** » – Lorsque plusieurs machines virtuelles commencent simultanément des analyses programmées, la puissance de traitement de la machine hôte risque d'être affaiblie, ce qui entraîne des problèmes d'utilisation et de performance sur l'hôte (voire son arrêt complet).
- « **Blitz de mise à jour** » – Semblable à un « blitz antivirus », le problème peut survenir lorsque toutes les machines virtuelles dotées d'une base de données de signatures locale tentent de télécharger et d'installer simultanément des mises à jour.

Failles de sécurité

Les machines virtuelles peuvent être déconnectées en toute simplicité et passer en mode veille pendant de longs intervalles. Au moment de leur remise en ligne (« réveil »), il se peut qu'elles présentent des failles de sécurité, telles que des vulnérabilités dues à des logiciels dépourvus de correctifs ou des bases de données de signatures de virus non mises à jour, que les cyber-criminels s'empressent d'exploiter.

Incompatibilité

Les machines virtuelles et physiques sont radicalement différentes, notamment au niveau de l'utilisation des disques non persistants et du processus de migration en direct des machines virtuelles, par exemple. Les programmes classiques de protection contre les logiciels malveillants, conçus pour des terminaux physiques, ont tendance à ne pas prendre en compte les caractéristiques virtuelles et physiques des machines, si bien qu'ils peuvent présenter des problèmes techniques imprévisibles, voire ne pas fonctionner du tout.

L'incompatibilité n'est pas une fatalité. La solution Kaspersky Endpoint Security for Business répond aux besoins des organisations qui choisissent d'utiliser la même solution basée sur un agent sur les infrastructures physiques comme virtuelles. Ainsi, Kaspersky Endpoint Security for Business est tout à fait capable de fonctionner de façon transparente et efficace dans les environnements virtuels. D'ailleurs, les ajustements spécifiques visant à optimiser les performances du système virtuel en font la solution idéale dans tous les environnements pour lesquels une solution basée sur un agent est recommandée.

L'ÉQUILIBRE

L'option basée sur un agent entrave considérablement les performances en termes d'efficacité en réduisant la densité des machines virtuelles et en affectant le retour sur investissement. Si la protection garantie par une approche de ce type est tout aussi efficace, les besoins en ressources, en revanche, restent très élevés et représentent un coût exorbitant pour la plupart des organisations ayant fait le choix de la virtualisation.

PROTECTION SANS AGENT

Les agents des logiciels de sécurité classiques consomment trop de ressources et manquent de flexibilité pour les machines virtuelles. Et s'il était possible d'assurer la sécurité des systèmes virtuels sans avoir à installer un agent au niveau des terminaux ?

C'est une solution envisageable si le système de sécurité est étroitement intégré à la plate-forme de virtualisation et qu'il peut faire appel à des fonctionnalités intégrées pour communiquer avec les machines virtuelles.

Dans ce cas, il est possible d'utiliser une seule appliance virtuelle distincte pour assurer la protection des machines virtuelles contre les programmes malveillants.

AVANTAGES

- La suppression du processus d'analyse sur les différentes machines virtuelles permet de réduire la quantité de mémoire totale nécessaire et de démultiplier ainsi les fonctionnalités du matériel physique tout en augmentant la densité de consolidation.
- Finie la vulnérabilité ponctuelle des systèmes au moment de la création d'une nouvelle machine dans la mesure où l'appliance de sécurité virtuelle se met elle-même régulièrement à jour.
- Étant donné que cette dernière est la seule à vérifier et à recevoir les mises à jour de la part du fournisseur de solutions de sécurité, il est relativement simple d'éviter les « blitz antivirus » et de limiter le taux d'utilisation des E/S.

CONTRAINTES

Si elle permet de bénéficier d'un meilleur retour sur investissement, il n'en reste pas moins que cette approche comporte un certain nombre d'inconvénients.

Un nombre limité de plates-formes supportées

L'approche sans agent se limite actuellement aux environnements VMware, pour lesquels la fonction de terminal vShield a été spécifiquement développée. Cependant, vShield présente quelques contraintes qui lui sont propres, ce qui restreint les niveaux de sécurité qu'il est possible de mettre en œuvre. La solution de sécurité proposée par vShield ne permet d'accéder malheureusement aux machines virtuelles qu'au niveau des systèmes de fichiers.

Protection plus restreinte

Sans un accès complet aux données et aux activités des machines virtuelles à partir d'une solution basée sur un agent, il n'est pas possible de protéger et de contrôler les terminaux.

Il serait préférable que les logiciels actuels de protection basée sur un agent comportent des modules de sécurité multi-niveaux, comme le contrôle des applications, le filtrage Web, la prévention des intrusions sur l'hôte (HIPS), un pare-feu personnel et bien plus encore.

Bien entendu, les performances d'un système de sécurité reposent sur la qualité des données relatives aux menaces et son moteur de protection contre les programmes malveillants. Qu'il soit basé ou non sur un agent, tout système de sécurité doit avant tout bénéficier de la meilleure solution de protection contre les programmes malveillants.

Mais en l'absence de toute approche multi-niveaux, il est indispensable que le moteur de détection des programmes malveillants soit aussi puissant que possible et qu'il dispose d'un maximum d'informations.

Il n'en reste pas moins qu'aucun moteur, aussi performant soit-il, ne peut offrir les niveaux de sécurité nécessaires dès lors qu'il est impossible d'accéder à la mémoire et aux processus des machines virtuelles. Les solutions sans agent conçues pour les environnements virtuels ont une portée plus limitée dans la mesure où elles ne proposent qu'une protection classique contre les programmes malveillants.

Gestion séparée des systèmes de sécurité

À l'heure actuelle, la plupart des organisations ayant fait le choix de la virtualisation ont conservé un double environnement, à la fois physique et virtuel.

Le déploiement de deux systèmes de sécurité distincts, un pour les machines virtuelles et un autre pour les machines physiques, implique l'utilisation de deux consoles d'administration séparées. Il convient ensuite de déployer les stratégies séparément dans les deux environnements et de fusionner manuellement les rapports pour bénéficier d'un aperçu global du niveau de la sécurité.

En ayant recours à deux systèmes parallèles gérés séparément, vous augmentez éventuellement les coûts en multipliant par deux les frais administratifs et en introduisant de nouveaux risques d'erreur.

Ce n'est toutefois pas toujours le cas. L'approche reposant sur l'utilisation d'une plate-forme unique et intégrée en matière de sécurité proposée par Kaspersky Lab permet d'intégrer de manière transparente les solutions de sécurité physique et virtuelle et de les gérer conjointement à partir d'une seule console.

L'ÉQUILIBRE

Parfois, l'option la plus efficace consiste à utiliser une solution sans agent. Par exemple, lorsque les activités de stockage et de gestion des bases de données sont prises en charge par des serveurs virtuels. Dans les environnements internes très sollicités où la densité des machines est essentielle et le niveau d'exposition aux menaces très limité, il est préférable d'avoir recours à une solution sans agent afin d'optimiser les performances.

Il convient toutefois d'évaluer minutieusement les risques. Lorsque la sécurité n'est assurée que par un moteur de protection contre les programmes malveillants, l'ampleur et la profondeur du niveau de protection qu'il propose ainsi que la qualité des informations relatives aux menaces qu'il exploite font bien entendu partie des critères les plus importants.

PROTECTION BASÉE SUR UN AGENT LÉGER

La sécurité des environnements virtuels basée sur un agent léger allie les performances d'une solution sans agent à l'approche de sécurité multi-niveaux proposée par les meilleurs systèmes de sécurité basés sur un agent.

Quand considère-t-on un agent comme « léger » ? Lorsque ses capacités se limitent aux seules fonctions nécessaires au niveau du terminal uniquement. Comme pour l'approche sans agent, les tâches les plus volumineuses sont effectuées par une appliance de sécurité virtuelle installée séparément. L'« agent léger » installé sur la machine virtuelle traite les charges de travail les moins lourdes de façon à atténuer au maximum son impact sur les performances des machines.

AVANTAGES

Sécurité multi-niveaux

La présence de l'agent léger permet désormais d'ajouter à la solution une couche de sécurité avancée au niveau des terminaux ainsi que des fonctions de contrôle, et notamment les suivantes :

Contrôles

Il est possible d'avoir recours à une « boîte à outils » de contrôles pour les terminaux.

- Il est possible de bloquer, de contrôler ou d'autoriser l'accès individuel à des applications spécifiques, ce qui restreint considérablement les risques d'infection par des programmes malveillants à partir de failles inconnues ou ne faisant l'objet d'aucun correctif, notamment dans le cas d'un scénario de blocage par défaut.
- Il est également possible de bloquer ou de contrôler des sites Web malveillants ou non liés à l'activité professionnelle afin de gagner en productivité et en sécurité, en contrôlant les activités en ligne non productives ou inappropriées.
- Il est possible de limiter ou de bloquer la connexion de certains périphériques, ce qui empêche tout téléchargement de programmes malveillants ou de données d'entreprise.

Technologies de sécurité supplémentaires

HIPS (Host Based Intrusion Prevention System) – Surveillance du système et du comportement réseau, et protection active contre les attaques visant la mémoire des machines virtuelles.

Un pare-feu hébergé sur l'hôte permet d'empêcher la diffusion de programmes malveillants en limitant l'accès réseau au niveau de la machine.

Les solutions reposant sur un agent léger sont en mesure d'interagir parfaitement avec les technologies de protection dans le cloud faisant appel à des méthodes avancées telles qu'AEP (Advanced Exploit Prevention) et BSS (Behavior Stream Signatures). Si la qualité du moteur de protection contre les programmes malveillants reste primordiale, les stratégies de sécurité virtuelle peuvent désormais faire appel à tout un arsenal de technologies disponibles pour les environnements informatiques physiques.

Efficacité des performances

L'utilisation d'une appliance de sécurité virtuelle distincte donne la possibilité aux entreprises de bénéficier de la plupart des gains de performance garantis par une solution sans agent.

- L'utilisation des E/S de l'hyperviseur, du processeur et de la mémoire est limitée. Les mises à jour sont effectuées par une appliance virtuelle unique et non par une multitude d'appliances installées sur chaque machine virtuelle, ce qui permet d'éviter tout risque de « blitz antivirus ». Si cette appliance unique est régulièrement mise à jour, les risques de vulnérabilité au niveau des machines sont également réduits dans la mesure où elles font l'objet d'une protection instantanée systématiquement à jour.

  Dans le cas de Kaspersky Security for Virtualization, cette mise à jour en continu, qui assure une protection instantanée contre les menaces grâce à la solution Kaspersky Security Network dans le cloud, est un processus particulièrement intensif. Il est donc indispensable de veiller à le centraliser.

- En mettant en œuvre des technologies de cache, il est possible de diffuser le résultat de l'analyse d'un fichier à l'ensemble des machines virtuelles sur l'hôte sans avoir à reproduire inutilement l'analyse. Vous bénéficiez ainsi de délais d'analyse beaucoup plus courts et d'une consommation des ressources plus limitée.

CONTRAINTES

L'agent est toujours là

Par définition, un système reposant sur un agent léger utilise toujours davantage de ressources qu'un environnement sans agent.

Gestion séparée des systèmes de sécurité

La plupart des solutions de sécurité virtuelle nécessitent l'utilisation d'une console distincte des autres composants.
Mais ce n'est pas toujours le cas. Nous aimerions d'ailleurs attirer votre attention sur l'architecture unique de la plate-forme centralisée de Kaspersky Lab.

Kaspersky Security for Virtualization a été conçu sur la plate-forme unique Endpoint Security for Business et fonctionne conjointement avec nos solutions de sécurité physique.

En d'autres termes, vous administrez votre sécurité virtuelle et physique avec une seule et même console même si vous disposez de deux solutions distinctes optimisées pour des environnements différents. Il est possible de créer et de déployer des stratégies conjointes, ainsi que de générer des rapports communs. La charge administrative supplémentaire reste très limitée voire inexistante et vous avez la possibilité de surveiller le système de sécurité de l'environnement informatique dans son ensemble de manière centralisée.

L'ÉQUILIBRE

Les solutions reposant sur un agent léger permettent de rétablir l'équilibre entre performances et protection en offrant le « meilleur des deux approches ». La présence d'un agent permet de déployer un niveau de sécurité avancé et des fonctions de contrôle au niveau des terminaux virtuels tandis qu'une appliance de sécurité distincte effectue l'ensemble des tâches pouvant être centralisées, ce qui évite ainsi toute redondance et minimise l'impact sur les performances.

À condition qu'elle soit conçue efficacement, une solution de cette nature s'avère généralement la plus intéressante dès lors qu'il est nécessaire de trouver le juste équilibre entre sécurité avancée et performances.

CONCLUSION

Les entreprises ont aujourd'hui pris conscience de la valeur proposée par la virtualisation, ainsi que des dangers que représentent les menaces, dont le développement est en constante évolution. Cependant, la mise en œuvre d'un système de sécurité inapproprié risque de nuire considérablement aux performances de vos systèmes virtuels et à votre degré effectif de protection.

La solution de sécurité idéale comble les failles des logiciels de protection existants en proposant une approche similaire à la virtualisation : flexible, adaptable et capable d'offrir régulièrement un important retour sur investissement ainsi qu'une excellente protection sans sacrifier les performances.

La mise en œuvre de Kaspersky Security for Virtualization vous permet ainsi de trouver cet équilibre parfait. En vous donnant la possibilité de mettre en œuvre les combinaisons d'applications de votre choix (agent léger, sans agent et à partir d'un agent), Kaspersky Security for Virtualization vous permet de bénéficier de la protection de notre moteur anti-malware, le « meilleur de sa catégorie », de tirer parti des avantages d'une conception adaptée à la virtualisation pour la garantie de performances optimales et de répondre à tous vos besoins en matière de sécurité via une approche unique de gestion intégrée.

En qualité d'experts reconnus à l'échelle internationale dans le domaine de la sécurité informatique, les équipes de recherche et développement de Kaspersky Lab ont créé une solution d'une grande flexibilité, capable de vous offrir les performances dont vous avez besoin et de sécuriser intégralement votre environnement virtuel grâce à son écosystème étendu.

L'exploitation du réseau Kaspersky Security Network et l'implication de nos équipes Global Research et Analysis Teams (GReAT) connues dans le monde entier nous permettent de bénéficier du plus vaste aperçu possible et de détecter les millions de menaces présentes aux quatre coins du monde. Grâce à cette veille stratégique, nous sommes en mesure d'identifier et, la plupart du temps, de prévoir les incidents de sécurité de façon à aider les entreprises à se protéger plus efficacement et à réagir plus rapidement si leurs systèmes informatiques sont compromis. Nous concentrons nos efforts sur la résolution des problèmes de sécurité informatique à l'échelle internationale, de la protection des infrastructures critiques à la prévention des fraudes et aux services de veille en passant par la mobilité des entreprises et la sécurisation des environnements virtuels.

Kaspersky Lab ne cesse d'anticiper et de prévenir les incidents menaçant la sécurité informatique des entreprises en réduisant les risques auxquels elles sont confrontées aujourd'hui et auxquels elles devront faire face à l'avenir.

À propos de Kaspersky Lab

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 16 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique et fournit des solutions de sécurité numérique efficaces aux grandes entreprises, PME et consommateurs. Kaspersky Lab, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 300 millions d'utilisateurs.

Plus d'informations sur kaspersky.com/enterprise

* Selon une enquête menée par IDC en 2012, l'entreprise occupe la quatrième place du classement par chiffre d'affaires des fournisseurs de solutions de sécurité des terminaux à l'échelle mondiale. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les fournisseurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.