KASPERSKY lab

PROTECTION DES ARCHITECTURES VIRTUALISÉES : COMPRENDRE LA DIFFÉRENCE

www.kaspersky.fr

PROTECTION DES ARCHITECTURES VIRTUALISÉES : COMPRENDRE LA DIFFÉRENCE

Êtes-vous prêts à adopter le virtuel ? Vous avez certainement pour objectif de tirer le maximum de votre infrastructure informatique. Exécuter simultanément plusieurs machines virtuelles sur un seul ordinateur au lieu d'utiliser des serveurs dédiés, qui ont besoin de puissance, de refroidissement et de maintenance, est certes un argument convaincant. L'alimentation de nombreux nœuds virtualisés par un seul serveur physique permet de réaliser des économies. La virtualisation peut avoir des répercussions économiques incroyablement puissantes : selon une étude menée par Forrester en 2011, la mise en œuvre d'une infrastructure VDI VMware permet d'obtenir jusqu'à 255 % de retour sur investissement ajusté en fonction du risque sur une période de 4 ans, avec un seuil de rentabilité à 17 mois après le déploiement.

La question est la suivante : combien de machines virtuelles pouvez-vous intégrer dans cette configuration sans impacter de façon notable les performances ? C'est ce qu'on appelle le « ratio de consolidation », et il s'agit d'un aspect très délicat de la virtualisation, qui nécessite la prise en compte d'une multitude de facteurs. Quel type de tâche vos machines virtuelles sont-elles supposées effectuer ? Quel logiciel hyperviseur utilisez-vous ? Que risquez-vous en mettant tous vos œufs dans si peu de paniers ? Et comment sécurisez-vous votre nouvelle infrastructure de manière fiable, en vous assurant de ne pas être vulnérables aux cybercriminels, sans pour autant tomber dans l'excès et ralentir les choses de manière considérable ? Afin de prendre la bonne décision, vous devez vous familiariser avec plusieurs concepts et étudier comment ils s'articulent.

Modèles de virtualisation

L'industrie a défini plusieurs modèles de virtualisation. Le présent document en aborde trois :

- **Virtualisation des serveurs** : permet à plusieurs instances d'un système d'exploitation de fonctionner en simultané sur un seul serveur. Il s'agit du meilleur moyen d'augmenter l'utilisation de vos ressources : jusqu'à 80 %, par rapport à un taux d'utilisation moyen de 10 à 20 % pour les serveurs physiques traditionnels à rôle unique[1].
  La virtualisation du serveur matériel, qui n'apporte qu'une couche intermédiaire (hyperviseur) entre la machine virtuelle et le métal nu, offre plus d'avantages que la **virtualisation du serveur logiciel**, où le système d'exploitation sous-jacent implique la consommation de ressources supplémentaires. Par conséquent, la priorité est donnée à la virtualisation matérielle pour la plupart des applications commerciales.

1 Ruest D. Virtualization.A Beginners Guide (Guide de découverte de la virtualisation). McGraw-Hill, 2010, Page 4

- **Virtualisation des postes de travail** : comporte des avantages différents en remplaçant une armée de postes de travail physiques par une infrastructure de postes de travail virtuels (**VDI**). Les « Clients légers » économiques, les postes de travail à distance basés sur le rôle, les agences distantes sans service informatique dédié et la maintenance de centaines de postes de travail sont pris en charge par une poignée de serveurs physiques.
- **Virtualisation des applications** : dans ce cas, contrairement à l'infrastructure de postes de travail à distance basés sur le rôle, un environnement virtuel n'est adopté que pour une seule application. Pour les approches de logiciel-service de plus en plus populaires, il s'agit d'un choix naturel, et efficace.

Chaque modèle de virtualisation peut être utilisé de nombreuses manières, et chaque utilisation comporte des risques. Parmi ceux-ci, le risque représenté par les cybermenaces est le plus menaçant, rendant indispensable l'utilisation d'une solution de sécurité. L'évaluation des risques devient encore plus difficile lorsque vous réalisez que ces trois approches peuvent être adoptées sur un seul réseau informatique. De plus, vous devrez également composer avec la consommation de davantage de ressources.

Il existe toutefois des méthodes permettant d'amoindrir l'impact sur votre nouvelle infrastructure virtuelle extrêmement efficace.

UNE SOLUTION DE SÉCURITÉ SPÉCIALISÉE POUR LES ENVIRONNEMENTS VIRTUELS S'AVÈRE ESSENTIELLE

Bien entendu, vous pouvez installer les agents de protection des terminaux traditionnels sur vos machines virtuelles. Mais cela comporte plusieurs inconvénients majeurs susceptibles de rendre l'expérience de votre infrastructure informatique virtualisée assez médiocre.

1. **Duplication.** Chaque machine virtuelle est dotée d'un ensemble identique de composants de sécurité, à savoir un moteur de protection contre les programmes malveillants isolé et des bases de données de signatures, qui devront être mis à jour de manière indépendante. De ce fait, une part significative de vos précieuses ressources (puissance de traitement, RAM et stockage sur disque) est inutilement consommée, ce qui réduit considérablement le ratio de consolidation qui en résulte.
2. **Les « tempêtes ».** Ce terme est utilisé lorsque plusieurs machines entreprennent des mises à jour des bases de données ou des analyses des programmes malveillants en simultané, ce qui peut engendrer une hausse soudaine de la consommation des ressources et, par conséquent, une chute des performances, voire un déni de service. La configuration manuelle permet de résoudre partiellement ce problème, mais avec des dizaines et des centaines de machines virtuelles, cette opération peut s'avérer extrêmement chronophage.
3. **Les brèches instantanées.** Certaines machines virtuelles demeurent à l'état dormant jusqu'à ce qu'elles soient activées en cas de besoin. Il n'est malheureusement pas possible de mettre à jour les bases de données ou les composants de la solution de sécurité sur une machine inactive. Ainsi, tout de suite après le démarrage et jusqu'à la fin de la mise à jour de sécurité, la machine virtuelle reste vulnérable aux attaques.
4. **Les « crises de panique ».** Une pratique courante chez les administrateurs système consiste à prédéfinir la réaction à une épidémie de virus en renforçant les paramètres de sécurité, en passant en mode « paranoïaque » et en déclenchant une analyse non planifiée. Une telle politique, qui peut s'avérer bénéfique pour les nœuds physiques, peut facilement causer l'arrêt d'un environnement virtuel.
5. **Problèmes d'incompatibilité.** Les machines virtuelles ont de nombreuses similarités avec leurs homologues physiques, mais il existe quelques différences majeures qu'il ne faut pas oublier, telles que l'utilisation de disques non persistants ou le processus de migration des machines virtuelles en direct. La protection contre les programmes malveillants traditionnelle, conçue pour les terminaux physiques, ne tient pas compte des spécificités des environnements virtuels, si bien que des problèmes techniques imprévisibles peuvent surgir, et les machines ne pas fonctionner du tout dans certains cas.

En raison de tout ceci, le besoin d'une solution spécialisée s'avère évident. Un tel produit devra être conçu en tenant compte de tous ces points, tout en apportant le niveau de protection le plus élevé et en ayant un impact minimum sur les performances globales. Kaspersky Lab, leader technologique dans le secteur de la cybersécurité, a toutes les cartes en main pour entreprendre cette tâche, et propose une solution adaptée aux trois plateformes de virtualisation les plus utilisées : VMware, Microsoft Hyper-V et Citrix.

PLATEFORMES ET MODES DE PROTECTION

Protection sans agent

VMware, l'une des premières plateformes de virtualisation à voir le jour, mais toujours la plus plébiscitée, propose une solution appelée vShield, qui déleste les machines virtuelles de la lourde tâche d'exécuter des bases de données identiques et de doubler les agents d'analyse des programmes malveillants. Cette approche est appelée « protection sans agent ».

Kaspersky Lab propose une solution de sécurité spécialisée pour les plateformes VMware : **Kaspersky Security for Virtualization | Agentless**. Dans le cadre de cette solution, les fonctions d'analyse sont transférées vers une appliance de sécurité virtuelle (SVA), une machine virtuelle spécialisée dotée à la fois des bases de données de sécurité et du moteur d'analyse, qui protège toutes les machines virtuelles fonctionnant avec l'hyperviseur.

Les avantages sont clairs :

- L'interface native offerte par VMware vShield permet d'accéder de manière efficace aux machines virtuelles, libérant ainsi les ressources de chaque machine et assurant la compatibilité avec les autres technologies VMware.
- Les ressources libérées en concentrant les fonctions de protection contre les programmes malveillants et de la base de données de signatures sur une seule appliance virtuelle peuvent désormais être utilisées pour déployer d'autres machines virtuelles, ce qui augmente le ratio de consolidation.
- Dès le démarrage de nouvelles machines, la SVA fournit une protection immédiate, sans « brèche instantanée » et sans avoir besoin d'installer d'autres logiciels.
- Toujours activée, la SVA de Kaspersky Lab met continuellement à jour sa base de données de signatures et, encore plus important, maintient la connexion avec le Kaspersky Security Network (KSN), une infrastructure mondiale qui traite les informations provenant de millions de participants volontaires et protège contre les menaces les plus récentes, avant même qu'elles ne soient déployées, à travers la mise à jour de la base de données.
- Le problème des « tempêtes » est éradiqué, car une seule SVA est mise à jour et analyse automatiquement les machines virtuelles, en suivant un programme défini de manière aléatoire et en limitant le nombre de processus utilisés.

En outre, grâce aux fonctions fondamentales de sécurité du réseau apportées par vCloud Networking and Security, la solution de Kaspersky Lab est capable de détecter et de prévenir les attaques à venir sur les machines virtuelles, en bloquant efficacement l'attaquant avec la technologie Network Attack Blocker[2].

2 Le paramétrage de la protection des réseaux dans KSV | Agentless requiert le déploiement d'une seconde SVA

Malheureusement, les capacités de vShield sont limitées, ne permettant d'accéder aux machines virtuelles qu'au niveau des systèmes de fichiers. De ce fait, les processus qui s'exécutent au sein de la mémoire de la machine virtuelle ne peuvent être surveillés et contrôlés par la protection sans agent contre les programmes malveillants. Cela signifie également que les autres technologies de protection des terminaux, telles que le contrôle des applications couplé à la création de listes blanches dynamiques, conçues pour apporter de puissants niveaux de sécurité supplémentaires, ne peuvent pas être mises en œuvre.

Il convient de noter que vShield étant une technologie propriétaire de VMware, le principe de protection sans agent permettant de sécuriser une infrastructure virtuelle ne peut être appliqué qu'à la plateforme VMware pour le moment.

Protection avec agent léger

Gardant à l'esprit les limites énoncées plus haut, **Kaspersky Lab** propose une autre solution pour la virtualisation, une approche intermédiaire entre la protection sans agent et avec agent complet : **Kaspersky Security for Virtualization | Light Agent**.

Tout comme la protection sans agent, les bases de données et le moteur d'analyse des fichiers se trouvent sur la SVA. Il y a toutefois une différence : un module résident léger est déployé sur chaque machine virtuelle protégée.

La solution Kaspersky Security for Virtualization | Light Agent n'est pas limitée par les fonctionnalités de sécurité de la technologie vShield et a directement accès à chaque machine virtuelle, y compris à tout ce qu'il se passe au sein de la mémoire opérationnelle. De ce fait, toutes les technologies de pointe de Kaspersky Lab peuvent être utilisées pour défendre l'infrastructure virtualisée.

Les principaux avantages de Kaspersky Security for Virtualization | Light Agent comprennent :

- Consommation réduite des ressources par rapport à une solution avec agent complet, car le moteur d'analyse des fichiers et les bases de données se trouvent sur la SVA dédiée.
- Compatibilité avec les trois plateformes de virtualisation les plus populaires : VMware, Microsoft Hyper-V et Citrix*.
- Niveau de protection le plus élevé possible, en ayant totalement accès aux ressources des machines virtuelles, notamment à la mémoire opérationnelle.
- Niveaux de sécurité proactive supplémentaires, tels que l'HIPS couplé à la prévention automatique des failles d'exploitation, et le contrôle des applications associé à la création de listes blanches dynamiques. Simple à déployer, même dans le cadre des scénarios de sécurité les plus stricts, notamment le « blocage par défaut ».
- Étant conçue pour la virtualisation, la solution fonctionne de concert avec les fonctionnalités uniques de l'environnement virtuel, et non contre elles.

Bien entendu, tout a un prix. La protection avec agent léger doit être présente sur chaque machine virtuelle nouvellement déployée, un processus facile à automatiser en incluant le client léger à l'image prégénérée de la machine virtuelle. En raison de la présence de l'agent léger, Kaspersky Security for Virtualization | Light Agent consomme davantage de mémoire que l'application sans agent ; mais il convient de dire que, dans certains cas, la solution de protection avec agent léger peut réellement surpasser l'application sans agent basée sur vShield.

Il est également important de garder à l'esprit que le nombre d'hyperviseurs compatibles se limite aux trois plateformes les plus populaires. Et, à l'heure où nous rédigeons ce document, la famille Microsoft Windows est le seul système d'exploitation invité compatible avec les applications sans agent et avec agent léger.

Cela ne signifie pas pour autant que vous êtes sans défense si vous n'utilisez pas l'une de ces trois plateformes. Vous pouvez toujours envisager de faire l'acquisition de la sécurité avec agent complet conçue par Kaspersky Lab.

Protection avec agent complet

Bien qu'il s'agisse d'une solution de protection avec agent complet, Kaspersky Endpoint Security est en fait capable de faire un travail remarquable dans les environnements virtuels. Bien qu'elle nécessite plus de ressources que Kaspersky Security for Virtualization, elle peut être utilisée dans les environnements virtuels. De ce fait, si vous avez besoin de sécuriser une configuration un peu particulière, qu'il s'agisse de serveurs Linux ou d'invités Windows sur un hyperviseur peu courant, vous serez toujours protégés.

Les avantages du déploiement de Kaspersky Endpoint Security sur votre infrastructure virtuelle comprennent :

- Compatibilité avec les systèmes d'exploitation les plus récents
- Incorporation de l'ensemble le plus complet de technologies avancées de Kaspersky Lab
- Principes de gestion parfaitement familiers, comme sur n'importe quelle machine physique traditionnelle
- Son efficacité est reconnue par les trois principales agences de conseils mondiales : Gartner, IDC et Forrester, qui ont récompensé cette solution trois fois comme l'une des meilleures plateformes de protection des terminaux actuellement disponibles.

Tableau 1 : Comparaison des fonctionnalités

Fonctionnalité	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Plateformes de virtualisation compatibles	VMWare	VMware, Microsoft Hyper-V, Citrix	Toutes, excepté au niveau du système d'exploitation[3]
Systèmes d'exploitation invités compatibles	MS Windows	MS Windows	MS Windows, Mac OS X et Linux
Ratio de consolidation au sein d'un seul hôte	* * *	* */* * *[4]	*
Administration centralisée avec Kaspersky Security Center	+	+	+
Fonctionnalité de KSN	+	+	+
Protection de nouvelles machines virtuelles sans installations supplémentaires	+	+/-[5]	-
Protection contre les programmes malveillants	* *	* * *	* * *
Pare-feu	-	+	+
Système de prévention des intrusions hébergé sur l'hôte (HIPS)	-	+	+
Prévention des intrusions	+	+	+
Contrôle des applications avec création de listes blanches dynamiques et prise en charge du blocage par défaut	-	+	+
Contrôle du Web	-	+	+
Contrôle des appareils	-	+	+
Gestion des systèmes	-	+[6]	+[6]
Chiffrement	-	-	+

Mais après tous ces savants calculs, la question se pose de nouveau : comment atteindre une efficacité maximale sans devenir vulnérable aux cybermenaces ? Il existe une méthode, que l'on pourrait qualifier de règle fondamentale, à savoir **la sécurité en fonction du rôle**.

3 La virtualisation au niveau du système d'exploitation, également appelée virtualisation en fonction de la zone ou du conteneur, emploie un mécanisme où plusieurs « conteneurs » d'espace utilisateur partagent un seul noyau du système d'exploitation. Parallels et Proxmox sont des exemples de ce type de plateformes.

4 Dépend de l'hyperviseur et du type de virtualisation.

5 Pour les machines virtuelles non-persistantes, la protection instantanée est disponible dès l'installation de l'agent léger dans l'image de la machine virtuelle. Pour les machines virtuelles persistantes, l'administrateur doit déployer l'agent léger manuellement.

6 Bien qu'elle soit offerte dans Kaspersky Security for Virtualization | Light Agent, la technologie de gestion des correctifs et d'évaluation des vulnérabilités consomme énormément de ressources et n'est par conséquent pas recommandée dans les environnements virtuels.

NE PARER QUE LES CONNEXIONS ENTRANTES ; UNE APPROCHE DE LA SÉCURITÉ EN FONCTION DU RÔLE

Chaque cybermenace qui menace vos terminaux physiques peut également menacer votre infrastructure virtuelle. Mais l'attaquant a absolument besoin d'une technique de pénétration de votre périmètre de sécurité afin de lancer une attaque. Par exemple, afin d'infecter un PC allumé, un cybercriminel peut leurrer l'employé pour le diriger vers le site Web malveillant, là où l'infection se produit en exploitant une faille dans le navigateur de la victime. Mais pour infecter un serveur de données profondément ancré dans une infrastructure informatique sans connexion Internet, il convient de trouver d'autres vecteurs d'attaque. Ainsi, si vous avez la certitude que seules les attaques au niveau du système de fichiers représentent une menace, si les données en question ne sont pas très importantes ou si vous utilisiez une VDI avec des politiques strictes sans accès au Web, vous pouvez opter pour une solution sans agent qui offre les avantages d'une protection instantanée, sans « brèche instantanée ».

Tableau 2 : Approche de la sécurité en fonction du rôle

Fonction	Accès externe	Valeur des données*	Valeur du service**	Conditions externes	Solution (Pourquoi telle solution doit être utilisée)
Serveurs dorsaux de bases de données	Non	Faible à moyenne	Moyenne à grande	Sauvegardes régulières	KSV | Agentless (données à courte durée de vie, moins de vecteurs d'attaque)
Serveurs Web frontaux	Oui	Faible	Grande	Relation de confiance avec plusieurs serveurs dorsaux	KSV | Light Agent (exposition possible aux dangers que représente l'accès public après une attaque réussie exploitant des éléments de confiance)
Application virtualisée ou VDI dédiée	Non	Moyenne à grande	Moyenne	Extrêmement limitées, pas d'installation d'application, pas d'utilisation de support de stockage amovible	KSV | Agentless (environnement prévisible, moins de vecteurs d'attaque)
VDI en remplacement des postes de travail	Oui	Moyenne	Moyenne	Utilisation de supports de stockage amovibles personnels, les utilisateurs disposent des droits d'installation	KSV | Light Agent (le besoin d'une sécurité renforcée est plus important que le besoin d'une réponse plus rapide. Plus de vecteurs d'attaque en raison de l'Internet public)
Serveurs Web de l'Intranet de l'entreprise	Oui	Faible à moyenne	Faible à moyenne	*Accès externe uniquement pour les utilisateurs autorisés utilisant des jetons physiques	KSV | Agentless (données de faible valeur pour l'entreprise, exposition très limitée à l'Internet public)

Fonction	Accès externe	Valeur des données*	Valeur du service**	Conditions externes	Solution (Pourquoi telle solution doit être utilisée)
Infrastructure de traitement des données du client	Oui	Grande	Grande	Besoin d'un environnement stable qui n'évolue pas ; contrôle des applications avec blocage par défaut recommandé	KSV | Light Agent (à des fins de conformité, des niveaux de protection supplémentaires s'avèrent absolument nécessaires)
Infrastructure test des développeurs Web	Oui	Faible à moyenne	Moyenne	Hyperviseur Linux et machines virtuelles invitées hétérogènes	KESB pour Linux, KESB pour Windows (données à courte durée de vie constamment renouvelées, plusieurs systèmes d'exploitation)

Le tableau ci-dessus donne quelques exemples qui permettent de comprendre le fonctionnement général des défenses en fonction du rôle. Il ne s'agit toutefois pas de recommandations directes concernant les rôles énumérés et ces informations ne doivent pas être utilisées en tant que telles. Chaque cas d'utilisation est unique ; il y a toujours de nombreux facteurs à prendre en compte et il est impossible de les synthétiser dans un seul tableau. Toutefois, afin de clarifier le concept, nous souhaiterions présenter les catégories Valeur des données et Valeur du service de manière plus détaillée :

- **Données de faible valeur** : ces données sont généralement dépersonnalisées, ne contiennent aucun secret gouvernemental, commercial ou personnel important, ou bien ont une courte durée de vie et sont constamment renouvelées. La perte ou l'exposition de ces données n'expose pas l'entreprise à d'importantes pertes commerciales et ne porte jamais atteinte à la réputation. Une base de données fonctionnelle dans laquelle les données de transition sont temporairement stockées constituerait un bon exemple.
- **Données de moyenne valeur** : ces données peuvent contenir des informations commerciales ou personnelles, sans toutefois être de nature financière ou médicale. Elles ne contiennent pas d'informations classées. La perte de ces données peut engendrer un dommage financier pour l'entreprise. L'exposition de ces données peut avoir un impact monétaire manifeste et porter atteinte à la réputation de l'entreprise, sans pour autant que cela soit vital. Exemple : données sur les clients d'un revendeur Internet.
- **Données de grande valeur** : peuvent contenir des informations financières et/ou personnelles sensibles ou des secrets commerciaux et représentent une part importante de l'avantage concurrentiel de l'entreprise. Elles peuvent également contenir des informations classées. La perte de ces données peut engendrer des pertes commerciales significatives et porter gravement atteinte à la réputation. L'exposition de ces données peut engendrer des sanctions financières, notamment des poursuites judiciaires, et porter atteinte à la réputation de manière irrévocable. Exemple : plans d'infrastructures critiques ou correspondance confidentielle de la direction.

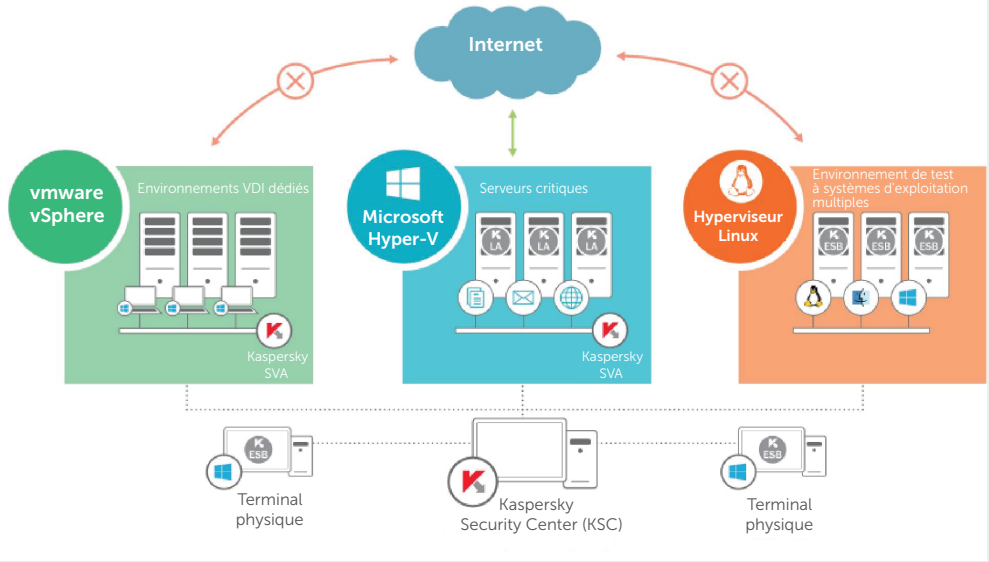
- **Service de faible valeur** : pas de tiers affecté, la vitesse de reprise des activités ne revêt que peu d'importance. Conséquences financières légères ou absentes en cas de dysfonctionnement. Probabilité d'atteinte à la réputation extrêmement faible. Exemple : portail d'informations de l'entreprise.
- **Service de moyenne valeur** : des tiers peuvent être affectés en cas de dysfonctionnement du service. La perte de ces données peut engendrer des dommages financiers manifestes. L'atteinte à la réputation est également manifeste et est intrinsèquement liée à la reconnaissance sociale du service : plus le service (ou le produit qui y est associé) est connu et populaire, plus les conséquences seront lourdes. Les données peuvent concerner une infrastructure gouvernementale, sans toutefois avoir une influence majeure sur le bien-être national. La vitesse de reprise des activités est d'une grande importance. Exemple : infrastructure VDI d'un intégrateur de systèmes qui fournit un environnement remplaçant les postes de travail parmi ses services.
- **Service de grande valeur** : des tiers sont presque assurément affectés. Le service est un élément clé de l'activité et peut également représenter un élément vital pour les activités des tiers. Possible influence sur le bien-être national. L'atteinte à la réputation peut s'avérer extrêmement préjudiciable et potentiellement irrévocable. La reprise des activités est de la plus haute importance ; si les activités ne sont pas reprises le plus rapidement possible, cela peut avoir des conséquences encore plus dramatiques. Exemple : infrastructure du système de surveillance vidéo du gouvernement.

C'est vous qui connaissez le mieux votre infrastructure et êtes à même de décider quelle sera votre sécurité ; les lignes directrices figurant dans ce document ne constituent qu'une méthode décisionnelle de base. Mais, oui, il est possible d'améliorer l'efficacité de l'utilisation de vos ressources et d'économiser l'argent de votre entreprise tout en sécurisant votre infrastructure virtuelle. N'oubliez pas toutefois qu'avant de déployer une solution de sécurité spécialisée, vous devez vérifier et adapter les paramètres de sécurité de base de votre réseau informatique. Un réseau proprement géré laisse moins de place aux vecteurs d'attaque et vous avez moins de chances d'être touchés en cas de problème.

EFFICACITÉ SIGNIFIE INTÉGRITÉ

La consommation efficace des ressources est une bonne chose, mais n'est rien sans un contrôle efficace. Vous pouvez certes déployer une solution sans agent d'un fournisseur pour vos serveurs dorsaux, une solution avec agent léger d'un autre fournisseur pour votre VDI et intégrer le contrôle des applications d'un troisième fournisseur pour une zone critique. Mais vous aurez ainsi trois consoles de gestion, trois ensembles de politiques à configurer et gérer, ainsi qu'un nombre important de mises à jour à appliquer à votre canal de données. Il serait certainement bien mieux de faire appel à un seul fournisseur, afin que toutes les mesures et tous les contrôles soient soigneusement organisés dans une seule console. Tous les produits de sécurité de Kaspersky Lab ont été conçus de sorte à être contrôlés de manière centralisée, via Kaspersky Security Center. Ainsi, vous pouvez gérer vos ressources virtualisées à partir de la même console que vous utilisez pour contrôler la sécurité de vos terminaux physiques.

L'application centralisée des mises à jour constitue un autre avantage. Vous n'avez pas besoin de télécharger les mêmes mises à jour pour chaque SVA sur chaque hyperviseur ; elles sont automatiquement déployées après avoir été téléchargées sur KSC.



La disponibilité des solutions de Kaspersky Lab pour les différentes plateformes de virtualisation est une autre fonctionnalité distinctive. Elle vous permet d'exécuter librement un environnement bien protégé à plusieurs hyperviseurs tout en profitant de la centralisation des contrôles dans le même KSC.

Figure 1 : l'environnement à plusieurs hyperviseurs doit être solidement et efficacement protégé

Par exemple, les composants fondamentaux de votre Active Directory (contrôleurs de domaine, systèmes de nom de domaine, etc.) peuvent être hébergés sur des serveurs virtuels Microsoft Hyper-V, employer une VDI Cirtix et comprendre des serveurs de bases de données fonctionnant avec VMware ESXi. Autrement, comme l'illustre la figure ci-dessus, vous pouvez opérer un environnement mixte contenant plus d'une plateforme d'hyperviseur et des terminaux physiques.

Dans ce cas, afin de bénéficier du meilleur équilibre entre performances et sécurité et de ratios de consolidation optimum :

- La VDI isolée dédiée peut être protégée par KSV | Agentless.
- L'infrastructure de serveurs, qui est essentielle pour l'entreprise et contient des données précieuses, doit être protégée par les niveaux de sécurité robustes de KSV | Light Agent.
- L'environnement de test, qui comprend l'hyperviseur Linux et de nombreux systèmes d'exploitation invités, ainsi que des terminaux physiques, est mieux protégé par Kaspersky Endpoint Security.

Dans tous les cas, les produits de Kaspersky Lab vous offrent la meilleure protection de l'industrie et vous permettent de choisir entre la facilité de déploiement et l'efficacité du retour sur investissement de la solution KSV | Agentless, la protection robuste de KSV | Light Agent ou toute autre combinaison au sein d'une seule infrastructure informatique.

Étant donné que Kaspersky Lab peut proposer des solutions de virtualisation avec agent, avec agent léger et sans agent, nous sommes en mesure de fournir des recommandations totalement objectives à nos clients. Nous ne faisons pas la promotion d'une technologie en particulier, mais mettons en avant la meilleure option ou combinaison d'options pour l'environnement d'un client particulier. Et puisque toutes nos solutions reposent sur le même moteur puissant de protection contre les programmes malveillants, et que nous les concevons toutes en tant qu'élément d'une plateforme de sécurité intégrée unique, nous savons que quel que soit votre choix, votre système virtuel sera efficacement sécurisé.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab, Moscou, Russie
www.kaspersky.fr

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

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

KASPERSKY lab