KASPERSKY SECURITY FOR VIRTUALIZATION

Une protection supérieure, flexible et efficace pour votre serveur et vos environnements de bureau virtuels

Les cas de violations de données impliquant des environnements virtuels coûtent en moyenne deux fois plus cher que les autres. Il n'est donc pas surprenant que les entreprises soient désormais très préoccupées par la sécurité des systèmes virtuels. Or, il est difficile de trouver une solution qui assure une protection efficace aussi bien pour les infrastructures de bureaux virtuels (VDI) en pleine croissance que pour les environnements de serveurs virtuels, tout en conservant les avantages de la virtualisation.

Étant donné que les terminaux virtuels et physiques sont exposés aux mêmes menaces de sécurité (car les cybercriminels ne font pas la distinction), vous ne pouvez pas vous permettre de faire de compromis sur la sécurité. Ni, bien entendu, sur les performances. Et c'est là que Kaspersky Security for Virtualization et son architecture unique entrent en jeu.

Kaspersky Security for Virtualization offre une exceptionnelle protection granulaire multi-niveaux destinée aux VDI et aux environnements de serveurs virtuels. Notre approche unique et simple ne compromet pas les performances de votre infrastructure virtuelle.

Points forts

UNE PROTECTION EXCEPTIONNELLE

- **Une protection multi-niveaux efficace pour toutes vos machines virtuelles (MV) contre les menaces connues, inconnues et avancées.**
- L'intégration au réseau Kaspersky Security Network (KSN) basé sur le cloud permet une protection proactive des VDI et des serveurs contre les menaces émergentes à l'échelle mondiale.
- Les contrôles des applications (listes blanches dynamiques, etc.), des appareils et de l'accès au Web permettent à l'administrateur d'appliquer des politiques de sécurité sur les VDI, au niveau d'un groupe de machines ou d'une machine unique, pour mieux protéger les utilisateurs sans compromettre leur productivité.
- La puissante association des technologies de blocage des attaques réseau (Network Attack Blocker), des pare-feu, des systèmes de prévention des intrusions hébergés sur l'hôte (HIPS) et des technologies anti-phishing protège vos machines virtuelles contre les attaques réseau.

MEILLEURES PERFORMANCES

- **Cette solution innovante brevetée[1] nécessite très peu de ressources, ce qui permet d'optimiser les ratios de consolidation pour une densité maximale.**
- La technologie de cache partagé élimine la nécessité de duplication des analyses, ce qui est particulièrement important pour les bureaux virtuels où de nombreux fichiers sont répliqués entre les machines.
- Les « blitz de mise à jour » et les « blitz antivirus » ainsi que les vulnérabilités ou les « clichés instantanés » sont éliminés.

vmware PARTNER TECHNOLOGY ALLIANCE
vmware READY NETWORKING AND SECURITY
CITRIX READY
VBLOCK READY

[1] Brevet des États-Unis Nº 9088618

EFFICACITÉ ACCRUE

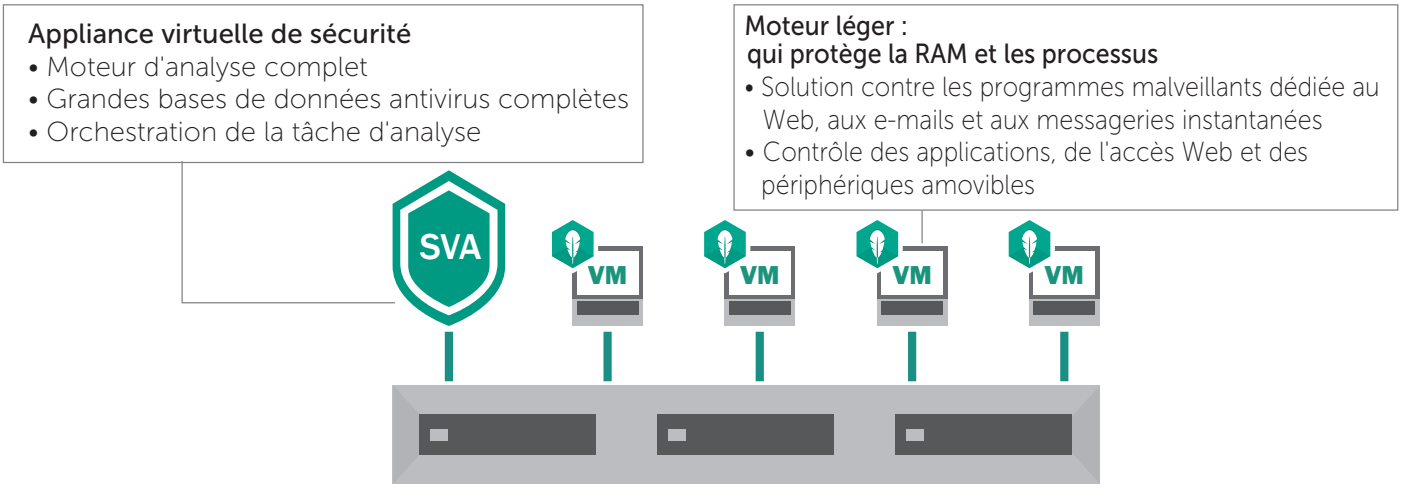
- **Pour commencer à protéger vos machines virtuelles, il vous suffit de déployer une seule appliance virtuelle de sécurité. Le déploiement d'un agent léger sur chaque machine virtuelle pour renforcer la protection est très simple et aucun redémarrage n'est nécessaire.**
- Une console unique permet de gérer ensemble toutes les machines virtuelles et physiques, ainsi que les appareils mobiles.
- L'utilisateur peut déployer et administrer de manière instinctive cette solution de protection, car les processus ressemblent à ceux des machines physiques, ce qui garantit une efficacité accrue et limite les erreurs de configuration.

FLEXIBILITÉ SUPÉRIEURE

- **Kaspersky Security for Virtualization prend en charge toutes les grandes plates-formes de virtualisation : VMware, Citrix et Microsoft.**
- Système de licences flexible : possibilité de choisir parmi plusieurs systèmes de licences basés sur le nombre de machines (postes de travail ou serveurs) ou de ressources (nombre de cœurs).

Technologie unique d'agent léger de Kaspersky Lab

MODE DE FONCTIONNEMENT ET AVANTAGES



L'architecture unique de Kaspersky Security for Virtualization protège efficacement les machines virtuelles sans sacrifier les ressources des terminaux. Vous verrez que vous obtiendrez des ratios de consolidation bien plus élevés qu'avec les solutions de lutte contre les programmes malveillants traditionnelles. Les « blitz de mise à jour » et les « blitz antivirus », ainsi que les vulnérabilités ou « clichés instantanés » sont également éliminés.

L'appliance virtuelle de sécurité de Kaspersky Lab analyse de manière centralisée toutes les machines virtuelles de l'environnement hôte. Kaspersky Security for Virtualization comprend un agent léger puissant qui est déployé sur chaque machine virtuelle[2]. Le déploiement de cet agent léger permet d'activer des fonctions de sécurité avancées sur chaque machine virtuelle, notamment le contrôle des applications, des périphériques et du Web, la protection contre les programmes malveillants pour la messagerie instantanée, les e-mails et le Web, ainsi que des méthodes heuristiques avancées.

Kaspersky Security for Virtualization offre ainsi une combinaison unique de protection multi-niveaux puissante et de performances efficaces.

Pour plus d'informations sur Kaspersky Security for Virtualization, contactez votre revendeur Kaspersky Lab local ou visitez www.kaspersky.fr

[2] Pour les machines virtuelles non persistantes, une protection instantanée est disponible après avoir été déployée une seule fois sur l'appliance virtuelle de sécurité. Pour les machines virtuelles persistantes, l'administrateur doit déployer l'agent léger au cours de l'installation.