Bitdefender® ENTERPRISE

LIVRE BLANC

La sécurité de nouvelle génération pour les datacenters virtualisés

INTRODUCTION

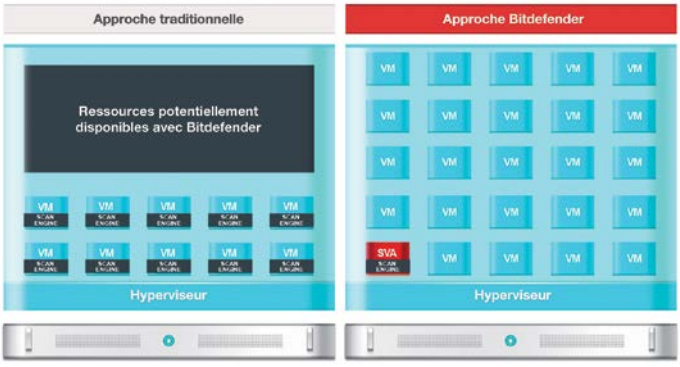
Ces dernières années, la virtualisation est devenue progressivement un élément stratégique clé pour le secteur informatique dans le monde entier et constitue désormais une approche éprouvée pour les environnements informatiques d'entreprise. Depuis son apparition en tant que technologie de consolidation, elle a continué à apporter d'énormes avantages opérationnels, qui aident à améliorer la souplesse et la productivité informatique des entreprises. La virtualisation permet de diminuer différents coûts associés à l'équipement et à la maintenance, tout en fournissant une meilleure disponibilité, des ratios de consolidation et des taux d'automatisation plus élevés dans les différents datacenters.

Pour bénéficier pleinement des avantages commerciaux liés à la virtualisation, les entreprises ne doivent pas négliger la sécurité. Bien qu'isolés et autonomes, les conteneurs virtuels sont vulnérables aux attaques malveillantes de plus en plus complexes fabriquées par des réseaux spécialisés de cybercriminels. Plus l'environnement virtualisé est grand, plus il est difficile de protéger efficacement les machines virtuelles, principalement en raison de leur nature dynamique : elles peuvent être déplacées d'un hôte à un autre, demeurer en sommeil ou rester hors connexion pendant de longues périodes. En plus de fournir une protection tenant compte du contexte, les outils de sécurité doivent également assurer une utilisation optimisée des ressources pour améliorer les performances dans l'environnement virtualisé.

LES LIMITES DES MODÈLES DE SÉCURITÉ TRADITIONNELS

Le besoin de logiciels de sécurité évolutifs, tenant compte du contexte, est encore plus crucial lorsque les entreprises adoptent des offres de cloud computing. Bien qu'il ne s'agisse pas de la meilleure pratique, certaines entreprises continuent à déployer des solutions antivirus traditionnelles pour postes de travail, conçues pour les plateformes physiques, lors d'une transition rapide des environnements physiques aux virtuels.

Ces solutions traditionnelles, ne prenant pas en charge la virtualisation ni son optimisation, ont prouvé leur inefficacacité et consomment beaucoup de ressources sur les machines virtuelles. Avec de lourds agents installés sur chaque machine virtuelle, les logiciels de sécurité pour postes de travail peuvent provoquer une dégradation récurrente et importante de la qualité de service pendant les processus d'analyse ou de maintenance.



Un exemple de ces dégradations de performances est le conflit de ressources ou "AV storm", qui a lieu lorsque de multiples machines virtuelles résidant sur le même hôte utilisent les ressources CPU et mémoire du serveur lors d'analyses simultanées. Outre la réduction de l'efficacité de la production, cette atteinte aux performances affecte également la capacité de mutualisation propre aux serveurs virtualisés.

UNE SÉCURITÉ SANS AGENT AVEC VMWARE VSHIELD™ ENDPOINT

En tant que leader mondial des infrastructures de virtualisation et cloud, VMware propose des solutions conçues pour les entreprises afin de constituer la clé de leur succès. Adoptée par des centaines d'entreprises renommées du monde entier, l'approche de VMware accélère la transition vers le cloud computing, tout en assurant un approvisionnement plus rapide, une plus grande disponibilité et une meilleure gestion. VMware améliore également les performances de la sécurité des VM avec Vshield Endpoint 5.

Conçu pour rationaliser l'utilisation des ressources et fournir des outils de sécurité efficaces pour datacenters virtualisés, VMware vShield Endpoint fournit l'API EPSEC pour une sécurité intégrée. Ce concept moderne offre un ensemble d'avantages technologiques qui aident à dépasser les limites de performances de la sécurité physique, tout en réduisant considérablement les besoins du système. Pour supprimer le besoin d'agents antivirus installés localement, les pilotes EPSEC transfèrent les fonctions antivirus clés vers une appliance virtuelle sécurisée dédiée. Les ressources physiques essentielles sont donc dédupliquées de sorte que les machines virtuelles n'aient plus à se livrer à une compétition acharnée pour obtenir les ressources disque et mémoire de l'hôte lors des phases d'analyses ou des mises à jour simultanées de signatures de virus.

Les avantages de vShield Endpoint :

- Rationalise le téléchargement des mises à jour antivirus et des événements de fichiers antimalwares sur une SVA sécurisée
- Améliore les performances des VM par des mécanismes de transfert sécurisés
- Permet d'augmenter les ratios de consolidation des VM en minimisant la prise de ressource de l'antivirus

Le tableau suivant illustre la différence en coûts/efficacité du point de vue de l'affectation des ressources de stockage entre les solutions intégrées à vShield et les logiciels antivirus traditionnels. Avec la sécurité sans agent, les administrateurs système peuvent facilement allouer une capacité de stockage par hôte physique plutôt que par VM, car il n'y a pas d'antivirus installé localement sur chaque machine virtuelle, et donc pas d'impact sur le stockage. Les calculs impliquent 4 000 serveurs virtualisés sur 400 hôtes physiques, avec un prix par To de SAN de 6 000 USD

Allocation de SAN avec les AV traditionnels	4 To (4 000 VM * 1 Go par VM)
Allocation de SAN avec vShield Endpoint	1,2 To (400 hôtes * 3 Go par hôte)
Coûts associés aux AV traditionnels	24 000 $ (4 To * 6,000)
Coûts associés à vShield Endpoint	7 200 $ (1,2 * 6,000)
Économies réalisées avec vShield Endpoint	16 800 $ (24 000 – 7 200)

Note : L'allocation de 3 Go de SAN avec vShield Endpoint comprend 2 Go pour la SVA et 1 Go pour la Console de sécurité.

Les failles de sécurité courantes se produisant avec les solutions de sécurité traditionnelles sont également supprimées en raison de l'intégration étroite de Security for Virtualized Environments by Bitdefender et vShield™ Endpoint.

Ce modèle de sécurité empêche les failles de sécurité dues à la latence au démarrage car les moteurs antivirus et la base de données résident dans l'Appliance Virtuelle (SVA) qui n'est jamais hors ligne. En effet, les moteurs d'analyse nécessitent généralement jusqu'à 12 secondes pour se charger, période pendant laquelle les machines virtuelles sont potentiellement exposées à toute menace.

Les agents antimalwares installés en local constituent une autre brèche exploitable. La plupart des attaques réussissent lorsqu'elles sont lancées sur des systèmes d'exploitation non patchés avec des signatures de virus non à jour. De plus, les agents antimalwares peuvent devenir eux-mêmes la cible de logiciels malveillants discrets qui tentent d'échapper aux contrôles de sécurité ou même de désactiver les programmes antivirus. Ces risques disparaissent complètement avec le modèle intégré à vShield.

Les composants Security Virtual Appliance et vShield Endpoint constituent un ensemble robuste de logiciels, qui implémente des capacités d'analyse centralisées tout en supprimant la prise de ressources de l'antivirus sur chaque machine virtuelle. Dans ce modèle à instance unique ou de sécurité sans agent, la connexion entre l'appliance Linux inviolable et les machines virtuelles protégées est intelligente et interactive, et ne laisse rien au hasard.

UNE SÉCURITÉ LÉGÈRE EN RESSOURCES POUR DATACENTERS VIRTUALISÉS

En réponse aux limites des approches de sécurité traditionnelles, **Security for Virtualized Environments by Bitdefender** fournit une protection extrêmement optimisée avec des besoins minimes en ressources, ce qui aide à prévenir tout goulet d'étranglement en cours d'utilisation. En répondant aux besoins en performances les plus importants, Bitdefender fournit une sécurité de virtualisation intelligente, sans affecter la mutualisation des ressources et les parcs de stockage.

L'excellence de la sécurité, ainsi que la simplicité et la souplesse globale fournie par Security for Virtualized Environments en font une solution idéale pour tout type d'infrastructure virtualisée. Tout en fournissant une protection silencieuse et une analyse du trafic extrêmement optimisée, la solution de Bitdefender s'adapte à la capacité des datacenters et améliore la capacité de production des entreprises en offrant de meilleurs ratios de consolidation.

Bitdefender tire davantage profit des solutions extensibles VMware en intégrant la Console de Sécurité à vCenter Server, un puissant outil d'administration pour les infrastructures vSphere. Cette association crée une ligne de défense étroitement surveillée dans les datacenters et offre une meilleure visibilité globale de la sécurité, tout en ouvrant la voie de façon dynamique aux modèles de cloud computing.

ÉTENDRE L'UTILISATION DE VMWARE VSHIELD POUR UNE SÉCURITÉ COMPLÈTE

L'analyse des processus et de la mémoire

Security for Virtualized Environments met non seulement en évidence l'avantage de VMware, mais renforce également la sécurité des VM en permettant l'analyse des processus et de la mémoire à l'intérieur du composant Silent Agent.

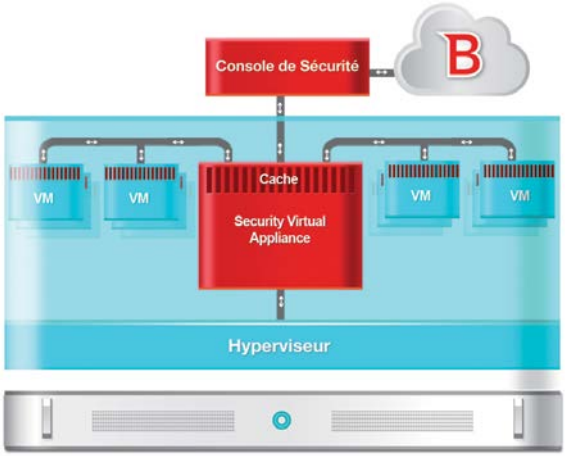
Avec des VM latentes exposées aux injections de rootkits sophistiqués, les analyses de la mémoire et des processus sont encore plus critiques que dans les environnements physiques. En plus de la rétention de l'activité antimalware dans la SVA, ces analyses locales garantissent une protection complète au niveau de la VM sans surcharger l'empreinte légère de Silent Agent.

Un support multiplateforme

Pour mieux tirer profit de la complexité et de la spécificité de chaque datacenter, Bitdefender apporte une valeur ajoutée à chaque projet de virtualisation en offrant un package complet adapté à toute technologie de virtualisation. Côté invité, les besoins système minimes sont associés à un support étendu sur différentes plateformes y compris Windows, Unix et Solaris.

Une architecture adaptée aux environnements non VMware

Dans les environnements non VMware, Security for Virtualized Environments by Bitdefender améliore la sécurité globale en incorporant des technologies dont les brevets sont en cours d'homologation, qui se comportent d'une manière similaire à vShield Endpoint. En raison de sa remarquable évolutivité, la solution Bitdefender est un facteur clé pour l'accroissement de la consolidation des ressources, permettant d'importantes économies dans les dépenses opérationnelles et la consommation de ressources. Basé sur une architecture extrêmement optimisée, Security for Virtualized Environments offre à chaque entreprise un ensemble d'outils de sécurité fiables capable de maximiser le retour sur investissements de l'infrastructure de bureau virtuel (VDI), sans compromettre les ratios de consolidation.



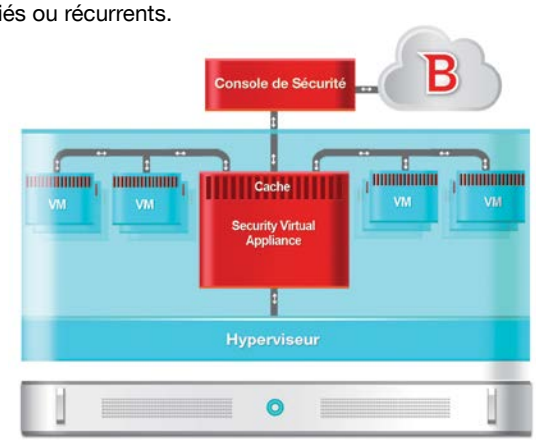
PRINCIPAUX COMPOSANTS DE SECURITY FOR VIRTUALIZED ENVIRONMENTS

Bitdefender fournit un package simplifié basé sur une architecture innovante comprenant :

Security Virtual Appliance (SVA) : Une machine de sécurité dédiée fonctionnant sur un serveur Linux sécurisé installé sur chaque hôte. Il s'agit d'un emplacement unique, centralisé, pour les moteurs d'analyse et les mises à jour de signatures de Bitdefender. Connectée aux invités protégés via les pilotes vShield EPSEC, SVA assure des analyses planifiées, à l'accès, et à la demande, et il déduplique la charge associée à l'antivirus. Elle est composée de quatre modules, qui se connectent directement à vShield Endpoint : de puissants moteurs d'analyse (intégrant les technologies proactives Bitdefender), une base de données de signatures, des gestionnaires d'analyse et des mécanismes de cache intelligents.

Silent Agent : Composant léger côté invité, qui affiche des notifications sur les événements de sécurité locaux et facilite l'analyse des processus et de la mémoire sur les machines virtuelles protégées. Il a une très petite empreinte (jusqu'à 4 Mo de disque et 6 Mo de mémoire) et peut être déployé automatiquement sur les systèmes invités Windows, Linux ou Solaris.

Security Console : une Interface Web intuitive agissant comme un hub de sécurité pour l'environnement virtualisé. Intégré à VMware vCenter server pour une meilleure visibilité, la console est le point central de l'administration et de la surveillance des VM protégées. Bitdefender Security Console permet le déploiement des Security Virtual Appliances et des Silent Agents, la gestion centralisée de la quarantaine, l'application de politiques via le datacenter virtualisé, la génération de rapports avancés sur l'état de sécurité disponibles sur le tableau de bord et la génération de rapports à la demande, planifiés ou récurrents.



CONCLUSION

La meilleure sécurité de sa catégorie, sans fioritures inutiles

A mesure que les entreprises virtualisent leurs infrastructures, les meilleures pratiques de sécurité ne doivent pas être oubliées. L'adoption de solutions traditionnelles s'est avérée inefficace en raison des différences d'architecture entre les environnements physiques et virtuels. Plus précisément, les performances des solutions logicielles traditionnelles ne sont pas suffisantes lorsque celles-ci fonctionnent sur des machines virtuelles. En plus de consommer inutilement de nombreuses ressources, elles peuvent avoir un impact négatif sur les performances comme des conflits de ressources.

Security for Virtualized Environments by Bitdefender

répond aux défis spécifiques de la virtualisation en fournissant une sécurité simplifiée et complète, même pour les datacenters hétérogènes les plus exigeants..

En s'associant à VMware, le leader mondial des technologies de virtualisation, Bitdefender propose une solution extrêmement optimisée, étroitement intégrée à vShield 5. Renforcé par les composants vShield Endpoint, Bitdefender met en place une analyse centralisée dans une appliance virtuelle Linux sécurisée. Tout en protégeant de façon non intrusive les machines virtuelles avec le Silent Agent, la solution va au-delà de la zone de protection de VMware en permettant des analyses de processus et de mémoire. De plus, elle couvre une large gamme de plateformes, y compris Windows, Unix et Solaris, dans des environnements fonctionnant avec toute technologie de virtualisation.

À PROPOS DE BITDEFENDER

Bitdefender est une entreprise internationale qui développe, édite et commercialise des solutions de sécurité dans plus de 200 pays. Sa technologie proactive, en évolution permanente, protège aujourd'hui plus de 400 millions d'utilisateurs dans le monde et est reconnue et certifiée par les organismes de tests indépendants comme l'une des plus efficaces et rapides du marché. Grâce aux équipes de R&D, d'alliances et de partenariats, Bitdefender a atteint l'excellence à la fois dans sa technologie classée n°1 et ses alliances stratégiques avec certains des fournisseurs de virtualisation et de technologie cloud leaders dans le monde. Depuis 2001, Bitdefender confie, pour la France et les pays francophones, l'édition et la commercialisation de ses solutions à la société Editions Profil.

À PROPOS DE VMWARE

VMware, leader mondial des infrastructures de virtualisation et de cloud computing, propose des solutions qui permettent aux entreprises d'entrer pleinement dans l'ère du cloud. Les clients s'appuient sur VMware pour les aider à changer la façon dont ils conçoivent, livrent et consomment les ressources informatiques en fonction de leurs besoins spécifiques et de façon évolutive. Avec un chiffre d'affaires en 2011 de 3,77 milliards de dollars, VMware compte plus de 350 000 clients et 50 000 partenaires. Basé dans la Silicon Valley, VMware dispose de bureaux partout dans le monde. Pour en savoir plus, consultez son site Web à l'adresse www.vmware.com/fr.