Bitdefender® ENTERPRISE

LIVRE BLANC

Protéger l'infrastructure virtuelle sans affecter les performances

Bitdefender

INTRODUCTION

La virtualisation présente de nombreux avantages, mais pose également des problèmes de performances quand on parle de sécurité. Cela suscite les questions suivantes : la sécurité de la virtualisation est-elle contre-productive ? Les solutions de sécurité disponibles actuellement ont-elles un impact sur certains des avantages apportés par la virtualisation ? Créent-elles des goulets d'étranglement et des problèmes supplémentaires dans les environnements virtualisés par rapport aux environnements de serveurs physiques ?

Ce document a pour objectif d'explorer certains des défis spécifiques à la sécurité de la virtualisation, de fournir les résultats de plusieurs tests de performances réalisés par Bitdefender et d'offrir un aperçu de la solution by Bitdefender (SVE).

LES LIMITES DE LA SÉCURITÉ DE LA VIRTUALISATION

Les solutions antimalwares avec agent, installées sur des machines virtuelles, pourraient ne pas être à jour en raison de l'inactivité d'une machine virtuelle hors ligne. Lorsque la machine virtuelle est redémarrée, la solution de sécurité doit se mettre à jour en téléchargeant ses dernières signatures antivirus et de moteurs, ainsi que les dernières mises à jour logicielles. Ce simple processus peut prendre entre 5 et 12 secondes, ce qui crée une opportunité pour les malwares.

Une alternative aux solutions antimalwares traditionnelles consiste à exploiter les solutions de sécurité intégrées à VMware Endpoint Security pour proposer une solution sans agent. L'approche sans agent réduit les problèmes de latence (boot latency) au démarrage et de protection antivirus non à jour. Cette approche présente toutefois des limites :

- VMware est actuellement le seul éditeur à proposer une offre sans agent via l'intégration à vShield Endpoint. Pour des entreprises utilisant des éditeurs avec hyperviseurs Xen ou Hyper-V, aucune solution sans agent n'est disponible. De plus, la solution sans agent est limitée aux environnements Windows. Les environnements Linux et non VMware ont toujours besoin de solutions traditionnelles avec agent.
- Bien que le terme "sans agent" soit utilisé, il n'est pas tout à fait exact. L'installation du pilote vShield Endpoint est nécessaire sur toutes les machines virtuelles à protéger.
- La solution sans agent présente également des limites, dans la mesure où seule l'analyse des fichiers est supportée. L'analyse de la mémoire et du registre, la surveillance comportementale et le contrôle du périphérique et des applications requièrent l'utilisation de solutions traditionnelles avec agent.

Le schéma ci-dessous présente la sécurité sans agent de Bitdefender via l'intégration à VMware vShield Endpoint Security. La solution Bitdefender a été développée pour sécuriser toutes les plateformes de virtualisation.

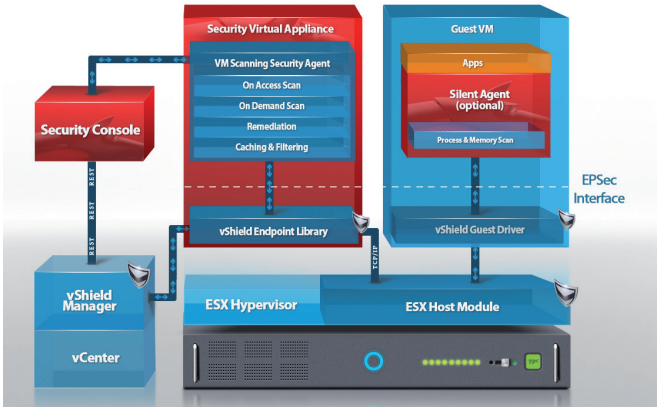


Figure 1: Security for Virtualized Environments - Intégration à VMware EPSEC

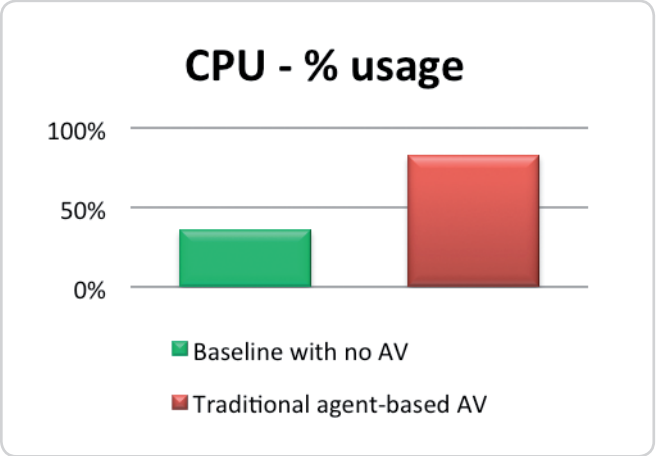
RATIOS DE CONSOLIDATION

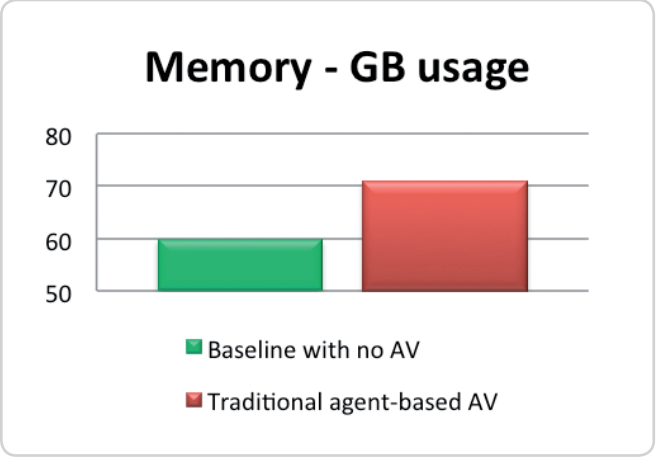
L'un des principaux avantages de la virtualisation sont les économies réalisées par les ratios de consolidation des machines virtuelles – atteignant le nombre maximal de machines virtuelles s'exécutant sur un hôte. Pour pouvoir avoir un impact minime sur l'environnement virtuel, les solutions de sécurité devraient être développées nativement pour la virtualisation, permettant ainsi des ratios de consolidation maximum des machines virtuelles.

La configuration matérielle requise pour un environnement virtuel peut varier de manière assez significative d'un environnement à l'autre ; elle dépend fortement des applications qui seront exécutées dans l'environnement virtuel. Les performances du processeur, de la mémoire, du réseau et du stockage doivent être considérées en fonction du type de machines virtuelles s'exécutant dans l'environnement.

Ainsi, un ratio de consolidation des machines virtuelles plus élevé sera obtenu avec des machines virtuelles d'applications web qu'avec des machines virtuelles exécutant des applications de bases de données. En fonction de l'application, il est recommandé d'allouer au moins 20% du pool de ressources système pour les pics d'utilisation.

Il convient de prêter également attention à l'impact qu'aura la sécurité sur l'environnement, comme le montrent les résultats des tests de performances suivants. Veuillez vous reporter à l'annexe pour des informations sur l'environnement de test.



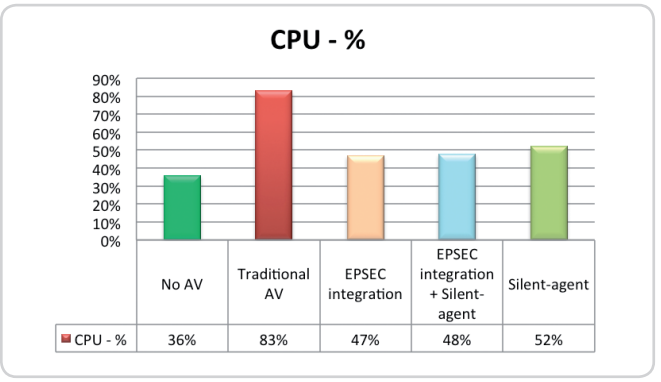


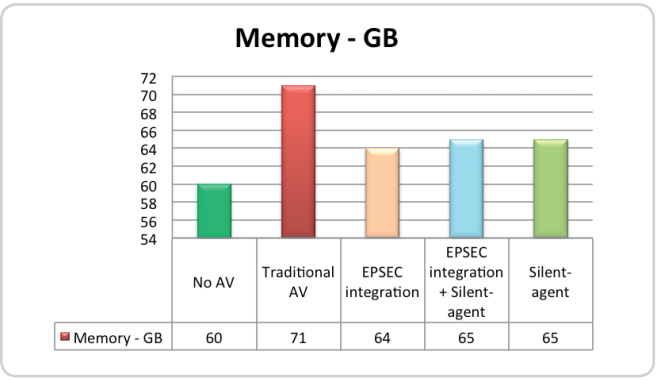
Le ratio de consolidation utilisé pendant les tests était de 45 machines virtuelles par hôte. Les résultats montrent qu'un antimalware traditionnel avec agent a un impact système de 131% sur le processeur et de 18% sur l'utilisation de la mémoire. Selon l'outil de calcul du coût par application de VMware (VMware Cost-Per-Application calculator), le coût moyen par VM s'élèverait à 1427€. Cependant, l'impact sur les performances causé par un antimalware traditionnel entraînerait l'achat de matériel supplémentaire, ce qui se traduit par un coût potentiel supplémentaire par VM avant même de prendre en compte le coût des licences de la solution antimalware.

Les mêmes tests ont été réalisés avec la solution Security for Virtualized Environments by Bitdefender, et les résultats des performances parlent d'eux-mêmes. L'utilisation du processeur et de la mémoire est indiquée pour les configurations suivantes :

- SVE dans une configuration sans agent s'intégrant à VMware vShield Endpoint Security (EPSEC)
- SVE dans une configuration sans agent s'intégrant à VMware vShield Endpoint Security (EPSEC) + SVE Silent Agent
- Uniquement SVE Silent Agent

De plus, SVE Silent Agent peut être utilisé dans tout environnement virtualisé, quel que soit l'hyperviseur utilisé.





D'après les résultats des tests de performances, on peut considérer que SVE permet d'avoir au moins 20% de machines virtuelles supplémentaires par hôte par rapport aux solutions antimalwares traditionnelles, quel que soit l'environnement virtualisé.

SÉCURITÉ DE LA VIRTUALISATION OPTIMISÉE

Security for Virtualized environments by Bitdefender est une solution conçue pour fonctionner dans tout environnement virtualisé, permettant aux clients d'obtenir des ratios de consolidation plus élevés par hôte par rapport aux solutions de sécurité traditionnelles. Des économies plus importantes sont générées concernant le matériel, le stockage et le refroidissement, et permettent ainsi aux clients d'augmenter le retour sur investissement de leur projet de virtualisation.

ANALYSE CENTRALISÉE QUEL QUE SOIT L'ENVIRONNEMENT VIRTUALISÉ

SVE est conçue comme une solution de sécurité hybride, adaptable aux datacenters mixtes et dynamiques actuels. Contrairement aux solutions de sécurité traditionnelles, Bitdefender réalise l'analyse centralisée en transférant une grande partie des fonctions antimalwares vers une appliance virtuelle sécurisée dédiée : Security Virtual Appliance (SVA). Cette méthode optimise à la fois les processus d'analyse à l'accès et à la demande, tout en dédupliquant les ressources informatiques critiques sur les serveurs hôtes. Pour permettre une protection complète, Bitdefender fournit des capacités d'analyse des processus et de la mémoire via Silent Agent, le composant SVE installé sur les VM.

Dans les environnements VMware, SVE fournit une sécurité sans agent via l'intégration avec vShield Endpoint Security (EPSEC). Pour les entreprises utilisant d'autres solutions de virtualisation (Microsoft, Oracle, Citrix…), Silent Agent garantit une protection optimale pour toutes les machines virtuelles sur lesquelles il est déployé.
Il existe deux versions de Bitdefender Silent Agent :

Silent Agent pour environnements VMware

- Dans les environnements Windows, Silent Agent est utilisé uniquement pour l'analyse de la mémoire, alors que l'analyse des fichiers système à la demande et à l'accès est gérée par le pilote vShield Endpoint. Il permet également l'intégration au Centre de Sécurité Windows.
- Il n'y a qu'un pilote installé par machine virtuelle, ce qui n'entraîne qu'une faible utilisation des ressources du système.
- L'impact sur l'hôte est minime grâce à l'utilisation du pilote vShield Endpoint et de Silent Agent. L'analyse à la demande de l'environnement est réalisée de manière séquentielle (VM par VM).
- Il fournit à l'utilisateur des informations sur l'état de la protection et l'historique des événements dans la VM.

Silent Agent pour environnements non VMware

- Comprend plusieurs pilotes pour effectuer des tâches d'analyse et de communication avec SVA.
- Fournit à l'utilisateur des informations sur l'état de la protection et l'historique des événements dans la VM.
- Utilise 20 Mo de mémoire.

DES PERFORMANCES AMÉLIORÉES PAR LES MÉCANISMES DE MISE EN CACHE

Security for Virtualized Environments by Bitdefender utilise un mécanisme de mise en cache unique, qui crée une liste blanche des applications et fichiers courants du système d'application. Ce processus améliore de façon significative les performances d'analyse des machines virtuelles et est mis à jour en continu. Cela est possible grâce à deux niveaux de cache utilisés par la solution. L'un d'entre eux est un cache d'auto-apprentissage, intégré à SVA. Silent Agent utilise un cache local pré-rempli en fonction des variables de son environnement. Il peut donc transférer l'analyse des objets requis, tout en excluant les objets qui sont sûrs.

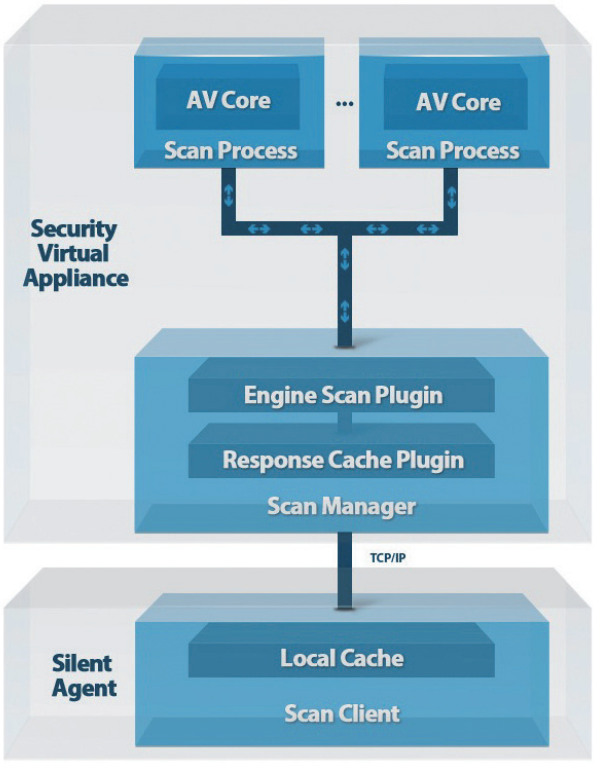


Figure 2 : Aperçu de l'architecture d'analyse

CONCLUSION

La sécurité en mode virtuel ne devrait pas nuire aux performances d'un environnement virtualisé et faire perdre de nombreux avantages de la virtualisation. Security for Virtualized Environments by Bitdefender résout ce problème par son approche unique de protection des machines virtuelles quelle que soit la technologie de virtualisation utilisée.

L'architecture de Security for Virtualized Environments by Bitdefender isole la fonctionnalité d'analyse des systèmes protégés, supprimant une grande partie des problèmes de sécurité de virtualisation présentés auparavant. De plus, la solution de Bitdefender aide à améliorer les performances de sécurité en employant des mécanismes de mise en cache de pointe. Cela génère des ratios de consolidation plus élevés dans les datacenters virtualisés, ce qui permet d'économiser des coûts de fonctionnement sans renoncer à la sécurité.

Pour plus d'informations, consultez www.bitdefender.fr/sve

ANNEXE

Les tests de performances ont été effectués sur le matériel et les plateformes de virtualisation suivants :

Spécifications matérielles	1HP ProLiant BL460c G7
	2 Xeon 6 CORE + HT @ 2.53 GHz (Intel Xeon E5649)
	144 Go de RAM
	Stockage 1,2 To PCI-E SSD iSCSI (10 Go)
Infrastructure VDI	20 Windows XP SP3 (32 bits), 1 Processeur, 1 Go de RAM
	20 Windows 7 (64 bits), 1 Processeur, 2 Go de RAM
	5 Windows 2k8 R2, 1 Processeur, 6 Go de RAM
Plateformes de virtualisation	Citrix XenServer 6.0 + XenCenter 6.0
	Citrix XenDesktop 5.5
	VMware ESXi 5.0 + vSphere 5.0

À PROPOS DE BITDEFENDER

Bitdefender est une entreprise internationale qui développe, édite et commercialise des solutions de sécurité dans plus de 100 pays. Sa technologie proactive, en évolution permanente, protège aujourd'hui plus de 400 millions de particuliers et d'utilisateurs professionnels dans le monde et est reconnue et certifiée par les organismes de tests indépendants comme l'une des plus efficaces et rapides du marché.

Depuis 2001, Bitdefender confie, pour la France et les pays francophones, l'édition et la commercialisation de ses solutions à la société Editions Profil.

PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender.

Bitdefender

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.