Bitdefender®

# La sécurité des environnements virtualisés sous Citrix Xen

La virtualisation permet aux entreprises de réaliser des économies importantes et leur apporte une grande flexibilité. Parmi les opérateurs de Datacenters les plus performants on compte des fournisseurs de services, tels que les fournisseurs de services cloud (également appelés IAAS “Infrastructure As A Service”) et les ASP - fournisseurs de services d’applications.

Au sein des entreprises classiques, la virtualisation fait évoluer le secteur vers un “IT as a service”. Lorsqu’une entreprise augmente le niveau de virtualisation de ses ressources et met en place des étapes afin de créer un cloud interne (privé), la marge opérationnelle devient le principal niveau de performances mesuré par les services informatiques. De même, la rentabilité et l’efficacité opérationnelle constituent les raisons principales de l’utilisation des clouds externes (publics).

De nombreuses entreprises utilisent l’hyperviseur Xen, alors que les fournisseurs de services optent souvent pour les systèmes d’exploitation Linux qui offrent des coûts et une souplesse de fonctionnement intéressants. Ces entreprises améliorent considérablement l’efficacité opérationnelle obtenue via l’utilisation innovante de la virtualisation puisque les datacenters font bien plus que de contribuer à ce business, ils constituent eux même ce business.

Lorsqu’elles sont en phase de création d’un datacenter avec un niveau élevé de virtualisation, les entreprises prennent normalement en compte l’impact prévisible en termes de matériel, de réseau, de stockage, de sauvegarde, etc. Elles doivent cependant également prendre en compte l’impact de la sécurité des postes de travail pour pérenniser leurs projets d’infrastructure cloud.

Cette présentation décrit l’impact souvent non anticipé de la sécurisation des postes de travail sur les marges d’exploitation, ce paramètre devant être pris en compte puisque les entreprises ont un recours croissant au cloud pour développer la virtualisation.

## Les défis de la sécurité de la virtualisation

Il est de notoriété publique qu’une solution antivirus est indispensable de nos jours. Les applications et les systèmes d’exploitation fonctionnant dans des environnements physiques, virtuels ou basés dans le cloud sont tous exposés à une éventuelle exploitation. Bien que la sécurité classique puisse être utilisée dans des environnements virtualisés, elle n’est ni conçue ni optimisée pour ce type d’infrastructures.

Utiliser des solutions antivirus traditionnelles peut provoquer des conflits spécifiques dans un environnement cloud tels que :

De faibles ratios de consolidation des machines virtuelles

Des latences au démarrage

Des “AV Storm” (conflits de ressources)

Des retards de mise à jour des antivirus sur les machines virtuelles inactives

Des goulets d’étranglement pour l’administration des VM

**Les ratios de consolidation** pâtissent conséquemment de l’utilisation d’une sécurité traditionnelle dans des environnements virtuels. Toutes les actions des applications et des utilisateurs effectuées dans l’instance d’une machine virtuelle sont analysées par l’agent de sécurité au sein même du système d’exploitation. Cela crée une importante duplication des processus au sein de l’environnement, des bases de signatures aux résultats d’analyse des mêmes fichiers, ce qui finit par entraîner des problèmes de performances et génère une baisse des ratios de consolidation des machines virtuelles.

**La latence au démarrage** est le résultat de l’utilisation d’une solution antimalware classique dans des environnements virtuels. Lorsqu’une machine virtuelle est lancée, la solution de sécurité doit télécharger les dernières signatures du moteur antivirus, ainsi que les dernières mises à jour logicielles. Ce processus de mise à jour peut prendre à lui-seul entre 5 et 12 secondes, ce qui crée potentiellement une opportunité pour le lancement d’attaques malveillantes.

Les phénomènes **d’‘AV Storm’** se produisent lorsque les agents de la solution de sécurité traditionnelle installés sur chaque machine virtuelle tentent au même moment d’effectuer une mise à jour ou une analyse planifiée. En procédant de cette manière, le processeur, la mémoire et l’IOP de l’hôte sont surchargés, ce qui entraîne de mauvaises performances de la machine virtuelle et, dans certains cas, peut conduire jusqu’ au déni de service.

**Un antivirus non à jour sur des machines virtuelles inactives** entraîne des problèmes cycliques de gestion des solutions de sécurité antimalwares traditionnelles. Les agents antimalwares installés sur les machines virtuelles inactives peuvent uniquement être mis à jour lorsque les machines virtuelles sont lancées, ce qui crée des problèmes de latence au démarrage et éventuellement des “AV Storm”, et ne permet pas à la machine virtuelle mal protégée de disposer des fichiers de signatures les plus récents.

**L’administration** des solutions de sécurité traditionnelles peut rapidement devenir délicate, en particulier dans le cas des déploiements les plus importants. À chaque fois qu’un nouvel agent classique est installé, il est enregistré auprès de la console d’administration. Lorsqu’une machine virtuelle est supprimée ou inactive, l’agent classique demeure indexé auprès de la console de sécurité et cette entrée ne peut être supprimée que manuellement.



CITRIX ready™

Bitdefender®

Cela peut devenir une tâche fastidieuse, notamment pour les grandes entreprises dans lesquelles les machines virtuelles sont fréquemment en mouvement.

Ce sont dans **les infrastructures VDI** (Virtual Desktop Infrastructure) que les entreprises font face à la plupart des défis mentionnés ci-dessus. Du côté des performances, une infrastructure VDI permet d'obtenir des ratios de consolidation bien plus élevés que la virtualisation du serveur. Il y a bien plus de copies d'agents antimalwares traditionnels, lesquels utilisent des ressources mémoire, processeur et de l'espace de stockage. Cela peut créer d'importants goulets d'étranglement en termes de performances, ce qui oblige les entreprises à choisir entre le succès d'un projet VDI (mesuré par son retour sur investissement) et la sécurité des postes de travail. Le caractère extrêmement dynamique des déploiements de VDI génère également différents problèmes d'administration, puisque des centaines d'instances de VM peuvent être créées, déplacées et détruites tous les jours.

**Une sécurité fiable :** les entreprises remettent rarement en question l'efficacité de leur solution de sécurité pour postes de travail, considérant qu'elle est "suffisante" et ignorant ses répercussions en termes de performances. Dans ce contexte, la virtualisation doit être considérée comme une opportunité d'évaluer les forces et faiblesse d'une solution de sécurité pour postes de travail. Lorsqu'elles adoptent des solutions spécifiques à la virtualisation, les entreprises doivent également prendre en compte le niveau de protection offert. De nombreuses solutions disponibles sur le marché ne disposent pas de fonctionnalités essentielles telles que l'analyse de la mémoire ou des processus des machines virtuelles, ce qui met en péril la sécurité des entreprises.

## Les défis de la sécurité de la virtualisation

Bitdefender a créé Security for Virtualized Environments (SVE) pour répondre aux besoins en sécurité des entreprises ayant des environnements extrêmement virtualisés. La solution centralise et déduplique l'analyse de machines virtuelles sur une Appliance virtuelle sécurisée pour chaque système hôte. Outre l'intégration à VMware vShield Endpoint 5 permettant une protection sans agents, SVE exploite les technologies uniques de Bitdefender pour protéger les VM fonctionnant sur des plateformes de virtualisation telles que Xen et Hyper-V.

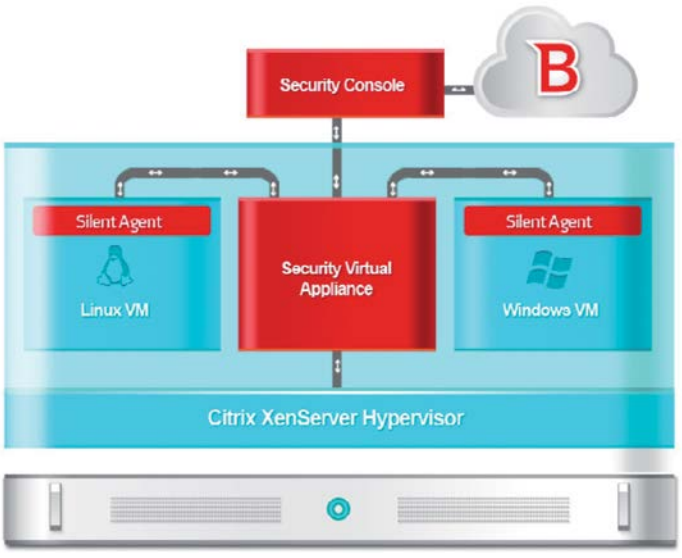


*Figure 1: Présentation de l'architecture SVE*

En exploitant la mutualisation des ressources SVE permet d'obtenir une meilleure densité des VM. Alors que les solutions classiques nécessitent que des clients antivirus soient installés sur chaque machine virtuelle, Bitdefender fournit une Appliance virtuelle dédiée permettant d'effectuer les activités antimalwares habituelles à l'extérieur des VM.

L'analyse centralisée évite d'avoir à installer un client antimalware classique complet, sur chaque VM. Cela économise des centaines de mégaoctets de stockage pour chaque VM ainsi que des ressources processeur, mémoire et réseau nécessaires pour le bon fonctionnement des agents antimalwares traditionnels. Des mécanismes de mise en cache intelligents améliorent encore les performances en garantissant que les fichiers dupliqués sur les VM (comme les fichiers de système d'exploitation) ne seront pas analysés plusieurs fois.

Pour assurer une visibilité complète et faciliter l'administration, SVE est intégré à Citrix XenCenter et VMware vCenter. SVE va même encore plus loin en s'intégrant à Amazon Web Services pour fournir une protection antimalware basée dans le cloud et délivrée en tant que service pour les utilisateurs d'Amazon EC2 du monde entier.

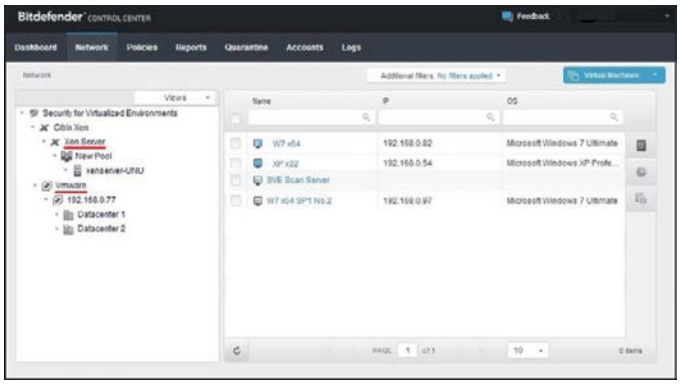


*Figure 2 : Un Centre de Contrôle/ une console de gestion unique pour Citrix et VMware*

Lorsqu'on souhaite en savoir d'avantage sur la technologie disponible, il est important de tenir compte du support de la plateforme de virtualisation et du système d'exploitation. SVE réunit dans une seule solution une grande souplesse dans ces deux domaines. À partir d'une console d'administration unique, les VM Windows et Linux fonctionnant sous Xen, vSphere, Hyper-V et KVM peuvent être protégées sans avoir recours à des agents antimalwares complets dans chaque VM. Cette approche indépendante de l'hyperviseur est importante aujourd'hui et sera amené à le devenir encore d'avantage à l'avenir, au fur et à mesure de l'adoption des nouvelles technologies du cloud par les entreprises. L'extrême souplesse de la technologie SVE a été mise en évidence par sa présence sur l'AWS Marketplace à son lancement.

Le déploiement revient simplement à importer deux appliances virtuelles. La Console de Sécurité est la console d'administration qui protège un environnement entier. Une seule Appliance de sécurité virtuelle est importée sur chaque hôte physique. Il s'agit d'appliances virtuelles Linux requérant une configuration minimale. Grâce à ce processus de déploiement simplifié même les plus grands environnements peuvent être protégés rapidement.

Avec Amazon Web Services, les instances protégées sont administrées de façon centralisée à partir de la Console de Sécurité Bitdefender, très intuitive en raison de son intégration étroite à l'API d'Amazon EC 2. Les utilisateurs de ce service bénéficient ainsi

d'une vue unifiée de l'état de sécurité de l'ensemble des régions AWS protégées, s'utilisant comme un point unique de contrôle pour la configuration et la génération de rapports sur les activités de sécurité au sein du cloud. Pour simplifier encore les tâches d'administration, la solution permet le déploiement automatique de la protection antimalware via le balisage d'instances AWS.

Enfin, SVE est la seule solution de sécurité de virtualisation capable d'analyser les processus et la mémoire des machines virtuelles. Cela, associé aux capacités antimalwares de pointe de Bitdefender, signifie que la sécurité n'a pas besoin d'être sacrifiée au profit des performances. Si les problèmes de performances causés par la sécurité peuvent compromettre les bénéfices attendus de la virtualisation, les problèmes de sécurité pouvant êtres inhérents à la virtualisation peuvent également limiter l'efficacité de la virtualisation dans une entreprise.

## Conclusion

Des nos jours les entreprises augmentent de plus en plus l'étendue de leurs projets de virtualisation. Alors que les premiers projets bénéficient naturellement de meilleurs rendements grâce à des solutions comme Security for Virtualized Environments (SVE), le passage à une plus grande utilisation de la virtualisation fait également augmenter les gains fournis par SVE. A mesure que l'utilisation de l'infrastructure en tant que service via un cloud privé ou externe devient plus courante, les stratégies employées par les fournisseurs de services les plus performants doivent être adoptées.

Choisir la sécurité adéquate pour postes de travail est un facteur clé de tous les projets de virtualisation en termes de performances et de sécurité. Les caractéristiques fondamentales de la sécurité des postes de travail dans les environnements virtualisés comprennent la capacité à centraliser et à dédupliquer l'analyse vers une Appliance virtuelle, ces avantages étant disponibles pour de multiples hyperviseurs et systèmes d'exploitation, avec intégration de l'administration. L'objectif principal est de proposer une sécurité fiable tout en minimisant la prise de ressources par la solution de sécurité sur les différents environnements tout en facilitant la charge d'administration.

## 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 CITRIX

Citrix (NASDAQ:CTXS) aide l'entreprise à transformer les pratiques de travail et de collaboration à travers le Cloud. Les solutions Citrix de virtualisation, d'infrastructure réseau et de Cloud Computing permettent de rendre l'informatique plus simple et plus accessible à plus de 260 000 entreprises. Les solutions Citrix sont utilisées par plus de 75 % des internautes chaque jour. Citrix dispose d'un réseau de plus de 10 000 partenaires répartis dans une centaine de pays. En 2011, Citrix a réalisé un chiffre d'affaires de 2,21 milliards de dollars. Pour en savoir plus : www.citrix.fr

ÉDITIONS PROFIL

**Plus de 400 millions d'utilisateurs** sont protégés par les technologies Bitdefender.

Bitdefender

Bitdefender est édité en France et dans les pays francophones par la société **EDITIONS PROFIL S.A,** spécialiste de la sécurité Internet et du filtrage de contenus numériques.