Bitdefender® ENTERPRISE

LIVRE BLANC

Les six choses les plus importantes à savoir sur la sécurité VDI/DaaS

Bitdefender

INTRODUCTION

La virtualisation se développant fortement, les entreprises cherchent de plus en plus à virtualiser les ordinateurs portables et de bureau. Des sociétés comme Citrix continuent d'améliorer les fonctionnalités de gestion, tandis que les fournisseurs de services, comme Amazon Web Services (AWS), continuent de créer et développer des offres d'hébergement de bureaux virtuels (DaaS). Mais la virtualisation n'est pas homogène. Le cloud public et le cloud privé sont des concepts différents, bien qu'apparentés, et il en est de même concernant la virtualisation d'un serveur et celle du système d'un utilisateur final.

Lorsque la virtualisation x86 a commencé à susciter un grand intérêt et que le retour sur investissement de ce modèle a été prouvé, l'adoption de la virtualisation des serveurs s'est rapidement accélérée. En revanche, la virtualisation des ordinateurs de bureau et des ordinateurs portables n'a pas suivi le mouvement. Les raisons de cette situation sont simples :

- Les serveurs, qu'ils soient physiques ou virtuels, restent dans le datacenter (le "cloud bursting" n'est pas encore une réalité).
- Les utilisateurs ont l'habitude d'utiliser des navigateurs pour accéder aux serveurs, et non d'y accéder directement, comme c'est le cas avec leurs postes de travail. Autrement dit, pour l'utilisateur, virtualiser un serveur auquel il a accès est transparent (l'infrastructure sous-jacente n'a pas d'importance dans son utilisation), tandis que virtualiser le poste de travail crée de profonds changements dans son mode de fonctionnement habituel.
- Les postes de travail doivent être transférés des mains des utilisateurs vers les datacenters.
- La principale motivation liée à la virtualisation des serveurs – le COÛT – n'est pas la même que celle liée à la virtualisation des postes de travail.

LES MOTIVATIONS DE L'ADOPTION D'ESPACES DE TRAVAIL VIRTUALISÉS

Comme David K. Johnson, chez Forrester, l'a justement fait remarquer "L'informatique modifie les raisons qui font qu'on s'intéresse à la technologie de virtualisation des clients. Il ne s'agit plus simplement de coût ou d'efficacité, mais de la flexibilité du mode de travail des employés !". Les principaux motifs de l'adoption de la Virtual Desktop Infrastructure (VDI) ont changé, ou peut être que ces motivations sont devenues plus rationnelles. Pour résumer, adopter une VDI en ayant comme objectif principal d'économiser en matériel et en maintenance est voué à l'échec.

L'IT modifie les raisons pour lesquelles nous nous intéressons à la technologie de virtualisation des clients. Il ne s'agit plus simplement de coût ou d'efficacité, mais de la flexibilité du mode de travail des employés !

Le problème réside dans la dernière lettre du terme VDI – Infrastructure, et le coût qui lui est associé. Là où la virtualisation du serveur était une transformation des datacenters, la VDI implique la création de nouvelles zones dans un datacenter.

La modification des habitudes de l'utilisateur final pose des problèmes. La plupart du temps, les utilisateurs finaux ont accès aux serveurs par l'intermédiaire d'un navigateur ou d'un client dédié, ce qui place l'interaction au niveau du poste de travail. Par contre, la VDI change cette donne. Les utilisateurs finaux doivent encore y avoir accès, mais cet accès passe désormais par un outil qui tient dans la main (tablette, portable léger, etc.) et un bureau à distance. L'interaction devient difficile (les gestes utilisés pour interagir avec des tablettes ne se transposent pas bien… en fait, une chose aussi simple à priori que de supprimer l'usage d'un clavier n'a pas été faite de manière adéquate !), de même pour la connectivité, la personnalisation et d'autres aspects des habitudes de l'utilisateur final. Pour résumer, la VDI ne se contente pas de modifier "l'aspect et le ressenti" de cette démarche, elle modifie la zone de confort et le comportement de l'utilisateur.

Toutes ces considérations à propos de la VDI sont en contraste avec la virtualisation des serveurs. Rétrospectivement, la virtualisation des serveurs semble simple. Elle engendre un bénéfice facile à comprendre (faire tourner sur un serveur de plus grandes charges de travail sur moins d'hôtes physiques), ne perturbe pas les utilisateurs (l'application Web aura exactement le même aspect), et procure d'autres avantages (flexibilité, redondance, etc.), pour des coûts qui étaient difficiles à atteindre en utilisant la technologie classique.

Tout ceci peut sembler démoralisant, mais la VDI, notamment utilisée en tant que DaaS, pourrait connaître une nouvelle avancée. Les architectes comme d'autres praticiens comprennent mieux que la VDI permet un contrôle centralisé des données, offre une meilleure flexibilité, et qu'il ne s'agit pas de faire juste des économies. On peut ajouter à cela la large adoption du BYOD ou, comme le proclame Citrix, la notion du "Ne possédez rien".

Ne rien posséder. C'est ce que j'entends souvent au cours de réunions avec des clients qui disent souhaiter ne plus avoir à gérer des datacenters sur leur site.[2]

La virtualisation des postes de travail est une démarche clairement différente, en termes de coûts et de bénéfices de celle de la virtualisation des serveurs. Qu'est-ce que cela signifie pour la sécurité des postes de travail ?

LA SÉCURITÉ DES POSTES DE TRAVAIL VIRTUALISÉS

Lorsque les entreprises se sont efforcées de virtualiser les serveurs, il s'est avéré qu'il existait dans les datacenters des zones qu'il allait falloir modifier. Le réseau, le stockage et les serveurs physiques eux-mêmes. Une actualisation de tout ce matériel était nécessaire pour s'adapter à la virtualisation. La manière dont les datacenters sont conçus, organisés, construits, gérés et dimensionnés a changé. Cependant, les applications tournant sur les postes de travail virtualisés peuvent rencontrer des difficultés et ne pas être aussi adaptées qu'il serait souhaitable.

Le passage du physique au virtuel est automatisé à tel point qu'on peut destiner un outil à un poste de travail classique et simplement attendre que le système d'exploitation et les applications qu'il contient soient transformés en machines virtuelles. La sécurité du poste de travail, c'est-à-dire la sécurité qui fonctionne dans un système d'exploitation, s'est révélée être la principale cause responsable des problèmes de performance dans les environnements hautement virtualisés. C'est parce que le passage du matériel au virtuel se passait en douceur jusqu'à ce que l'on se rende compte que les problèmes de performance étaient dus aux solutions antivirus classiques. On ne se posait simplement pas la question de savoir si tout ce qui tournait dans une VM pouvait être virtualisé de manière optimale.

Même si la virtualisation des serveurs a pour résultat positif de disposer de ratios de consolidation intéressants (c'est-à-dire, d'un nombre de serveurs pouvant tourner sur chaque matériel plus élevé), ces ratios sont bien inférieurs à ceux réalisables via la VDI. Chaque poste de travail virtualisé nécessite nettement moins de ressources de l'hôte qu'un serveur virtualisé. Ainsi, beaucoup plus d'instances de VDI peuvent exister par CPU, allocation de RAM, etc.

Le problème est que la sécurité du poste de travail qui fonctionne dans chaque système est virtualisée comme faisant partie de la VM, mais est aussi dupliquée sur toutes les VM. Dans le cas de l'utilisation d'un antivirus classique pour postes de travail, chaque VM doit gérer un ensemble de moteurs d'inspection, de bases de données heuristiques, de signatures et tout ce qui est associé à la sécurité du poste de travail. Les agents antivirus avaient été conçus pour tourner sur des supports matériels uniques suivant le modèle traditionnel, et non sur du matériel partagé qui offre des avantages dans les environnements virtualisés.

Le résultat est communément qualifié de "antivirus storm", qui provoque notamment des goulets d'étranglement de la performance dus à :

- Des analyses programmées au cours desquelles l'agent antivirus de chaque VM tente d'utiliser le maximum de ressources matérielles disponibles, ce qui épuise rapidement ces ressources.
- Des mises à jour au cours desquelles chaque agent antivirus doit télécharger localement les dernières signatures et moteurs heuristiques pour maintenir la sécurité à son niveau optimal.
- Des mises à niveau au cours desquelles les moteurs antivirus sont modifiés ou réinstallés pour maintenir la sécurité à son niveau maximal de mise à jour.
- L'analyse des mêmes objets (fichiers, registres, etc.) sur des VM de modèles identiques, partageant donc des mêmes versions de nombreux objets communs.

Les outils d'administration des solutions antivirus classiques apportent leur lot inhérent de problèmes dans les environnements virtualisés. Comme mentionné, la flexibilité est un bénéfice clé de la virtualisation. Le déplacement des VM d'un hôte à l'autre à la demande, les cycles de maintenance, etc. en font partie. Ceci signifie aussi pouvoir créer et détruire des VM, notamment des instances VDI, à volonté. Les outils d'administration traditionnels sont conçus pour surveiller et contrôler des clients antivirus sur des systèmes très statiques et ayant une longue durée de vie. Si des centaines, voire des milliers de VM sont créées et détruites quotidiennement, ces consoles sont rapidement submergées par des entrées orphelines.

LES SIX CHOSES LES PLUS IMPORTANTES À SAVOIR SUR LA SÉCURITÉ VDI/DAAS

Même si les entreprises ne vont pas toutes rencontrer de difficultés avec les solutions antivirus traditionnelles en se lançant dans la virtualisation des serveurs, chaque déploiement de VDI créera des problèmes dès le départ. Au bout du compte, les clients antivirus et les outils d'administration classiques sont inadaptés aux environnements virtualisés. Malheureusement, il arrive que des entreprises soient dans l'obligation de décider d'arrêter un projet VDI ou que des instances VDI soient créées sans protection des postes de travail. Aucune de ces perspectives n'est acceptable.

Compte tenu des caractéristiques clés de la virtualisation, une solution antimalware conçue pour des environnements virtualisés, devrait posséder, au minimum, les propriétés suivantes :

1) Des composants centralisés et dédupliqués

La première source des problèmes de performance est l'architecture des systèmes d'application. Dans les environnements traditionnels, chaque poste de travail était un îlot physique et les clients antivirus étaient conçus dans cet esprit. Dans les environnements virtualisés, exécuter un client antivirus complet et indépendant dans chaque VM, notamment dans le cas des VDI, va conduire à d'importants problèmes de performance.

Supprimer les composants d'analyse des VM et les déplacer vers des appliances virtuelles basées sur Linux réduit considérablement l'impact de l'antivirus pour postes de travail. Pour effectuer une inspection à partir d'une appliance virtuelle, une méthode d'inspection à distance doit être disponible.

Il faut rechercher un éditeur capable de prendre en charge l'analyse sur des plateformes multiples pour tous les types de postes et de systèmes d'exploitation. Il est quelquefois difficile de comprendre ce qu'un produit est capable de prendre en charge exactement, et sur quels postes de travail. De nombreux fournisseurs ont intégré VMware vShield Endpoint, qui n'est compatible qu'avec les hyperviseurs ESXi, et ne protège que le système de fichiers et les VM Windows.

Centraliser les résultats d'analyses et les informations associées est également important. Par exemple, si un fichier est analysé sur une VM d'un hôte, il ne devrait y avoir aucune raison d'analyser le même fichier sur d'autres VM protégées par une appliance virtuelle. Il est fort probable que les groupes de VM exécutent les mêmes tâches (de nombreuses instances de VDI basées sur un ou deux modèles, par exemple).

2) Une empreinte minimale dans la VM

Le terme commercial "sans agent" s'est beaucoup répandu, mais il peut induire en erreur. Il doit y avoir un logiciel dans chaque VM pour faciliter l'analyse à distance avec une appliance virtuelle.

Comme avec VMware vShield Endpoint, ce logiciel doit être joint à un autre package (VMware Tools), ou constituer lui-même un package créé par le fournisseur de sécurité. Il faut noter qu'avec vShield Endpoint, il n'existe pas d'interface utilisateur graphique (GUI) dans les VM protégées, et l'analyse de la mémoire et des processus n'est pas supportée. Il existe des packages supplémentaires proposés par des éditeurs de sécurité pour ajouter des fonctionnalités supplémentaires sur vShield Endpoint. Dans certains cas, l'éditeur peut proposer un package qui remplace entièrement vShield Endpoint.

Le terme marketing "sans agent" s'est beaucoup répandu, mais il peut induire en erreur. Il doit y avoir un logiciel dans chaque VM pour faciliter l'analyse à distance avec une appliance virtuelle.

Le niveau minimal de fonctionnalités requis pour une introspection à distance efficace doit exister dans chaque VM. L'objectif est de centraliser le plus possible, de réduire les mises à jour / mises à niveau nécessaires à la VM. Cependant, certaines fonctionnalités doivent être conservées dans la VM. L'antimalware ne nécessite que certains blocs d'un fichier pour fonctionner. Cette inspection dépend du type de fichier et d'autres informations qui ne peuvent être connues qu'après la décompression. Par conséquent, il est logique d'inclure des moteurs qui décompressent et recompressent les fichiers au sein de chaque VM. Si la décompression est pratiquée sur l'appliance virtuelle, les fichiers entiers doivent êtres transférés vers l'appliance virtuelle via le réseau.

3) Une amélioration tangible de la performance

Comme le dit l'adage "la confiance n'empêche pas le contrôle". N'hésitez pas à rechercher des informations sur les performances répondant aux normes des outils utilisés dans l'industrie, par exemple Login VSI (http://www.loginvsi.com/). Les résultats des tests effectués à partir d'outils personnalisés peuvent être trompeurs. Dans la mesure du possible, essayez de vérifier dans votre propre environnement les informations concernant la performance. Et surtout, vérifiez le modèle utilisé pour déporter les analyses dans la pratique, car certains fournisseurs prétendent que l'analyse déportée fonctionne dans différents environnements, alors qu'elle est en fait limitée aux hyperviseurs ESXi et aux VM Windows, ce qui implique de recourir à un agent antivirus classique (et donc 'lourd') dans toute configuration n'entrant pas dans le cadre restrictif des environnements supportés.

4) Une intégration de l'administration

Les antivirus traditionnels des postes de travail s'intégraient à Active Directory. Si cette intégration doit toujours être présente quand on a affaire à des postes traditionnels, l'intégration aux systèmes d'administration de la virtualisation est une nouvelle norme. VCenter et XenServer en sont les exemples les plus connus, alors que l'intégration à Amazon Web Services pour protéger les instances Amazon Machine Images, ou d'autres consoles de cloud public, peut également se révéler nécessaire.

L'intégration doit être en mesure de maîtriser la création ou la suppression de VM, permettre l'application de la politique de sécurité en fonction des catégories (groupes de VM, de Pools de ressources, etc.), et fasse en sorte globalement que les tâches de gestion effectuées dans la console d'administration de la virtualisation soient visibles dans la console de gestion de la sécurité.

5) Une compatibilité avec tous les environnements

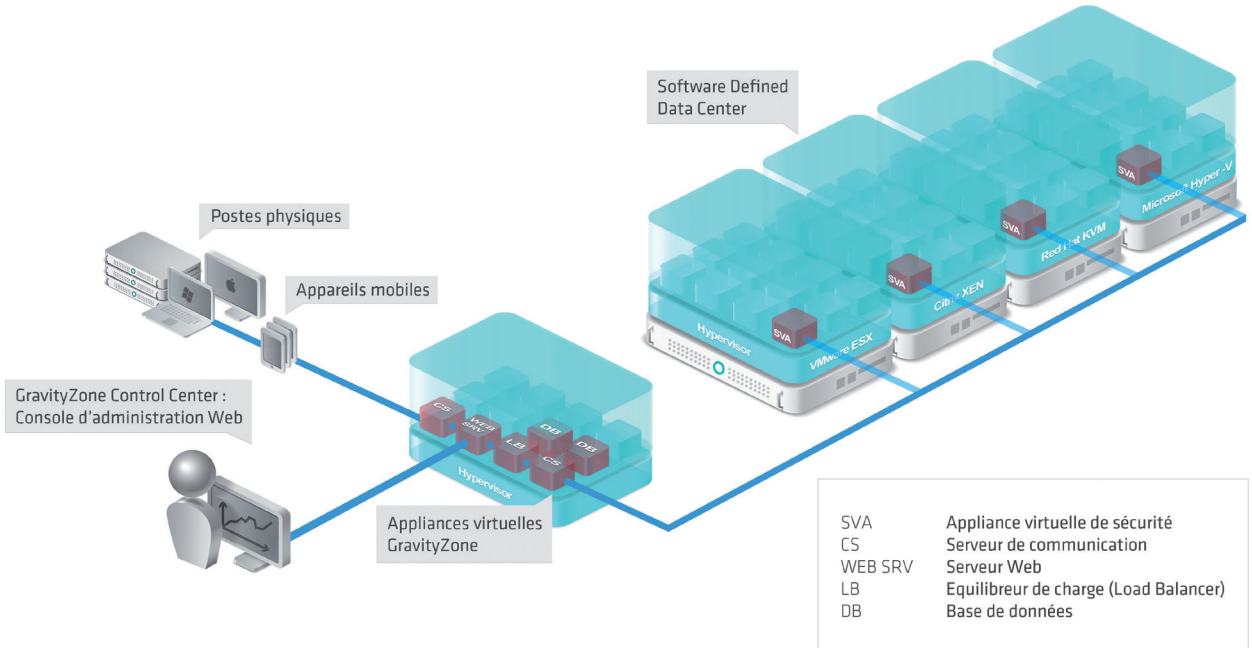
Même si l'environnement VMware ESXi est le plus répandu aujourd'hui dans les entreprises, le marché au sens large est beaucoup plus diversifié. Par exemple, les solutions Citrix, comme XenDesktop et VDI-in-a-Box, peuvent gérer des VM tournant sous Xen, ESXi et Hyper-V. En déployant une VDI, une entreprise possédant un datacenter axé sur VMware peut développer la base ESXi pour inclure une VDI gérée par Citrix. Cependant, une petite ou moyenne entreprise peut préférer utiliser Hyper-V ou Xen en Open source pour faire des économies, ou parce qu'elle ne possède pas de déploiement VMware.

Les prestataires de services qui élaborent des offres de DaaS peuvent également se tourner vers des hyperviseurs alternatifs, comme Xen ou KVM, pour des raisons de coûts.

Différents types de scénarios existent aujourd'hui, mais aucune entreprise ne souhaite dépendre d'un seul fournisseur d'infrastructure. C'est la raison pour laquelle il est important de faire appel à des fournisseurs dont les solutions de sécurité sont compatibles avec un grand nombre d'environnements.

6) Une protection de multiples types de postes de travail

Régler la question de l'antimalware pour postes de travail dans des environnements virtualisés est important, particulièrement dans le cas des VDI. Cependant, introduire une nouvelle console autonome en tant que solution ponctuelle n'est pas recommandé. Les éditeurs devraient être capables de proposer l'administration et le contrôle des environnements virtualisés dans la même console que celle utilisée pour gérer des postes de travail classiques et les postes mobiles. Bien qu'il existe chez certains la possibilité d'envoyer des journaux à une console centrale de reporting, cela ne permet pas nécessairement de disposer d'un contrôle centralisé. Méfiez-vous des solutions qui réclament de multiples points de contrôle dans un seul environnement pour diverses raisons officielles (fonctionnalités spécifiques, taille du parc à administrer au global, etc). Préférez les solutions qui possèdent des consoles de gestion modulables et évolutives, quelle que soit la taille et/ou la distribution de votre environnement.



L'APPROCHE BITDEFENDER POUR LA PROTECTION DES VDI

Bitdefender a choisi une approche polyvalente pour protéger les déploiements VDI. L'analyse déportée, centralisée et dédupliquée est un élément clé du mécanisme de protection, tandis que fournir une console d'administration puissante et évolutive permet de relier entres eux les VDI, la virtualisation du serveur, les postes de travail traditionnels et les postes mobiles.

L'architecture de la solution de gestion de sécurité GravityZone est fondée, non sur l'architecture client-serveur classique, mais plutôt sur des technologies cloud. A partir du datastore persistant, Bitdefender exploite MongoDB (https://www.mongodb.org/), un datastore non-relationnel, évolutif et offrant de haute performance.

GravityZone est fourni en tant qu'appliance virtuelle unique qui est importée dans un environnement virtuel. L'appliance est clonée autant de fois que nécessaire, chaque instance jouant un ou plusieurs rôles discrets, comme celui de base de données ou de console Web d'administration, au sein d'un unique déploiement. Avec un système de redondance intégré, qui inclut la répartition des charges logicielles, un seul déploiement permet de gérer toutes les évolutions horizontales requises et de couvrir les différents lieux à protéger.

GravityZone possède trois modules de protection principaux, vendus sous forme de licences séparées, mais administrés (gestion et contrôle) par la même console Web. Ces modules sont Security for Endpoints (pour les postes de travail classiques), Security for Virtual Environments, et Security for Mobile.

Security for Virtual Environments (SVE) fournit une analyse déportée, centralisée et dédupliquée pour un grand nombre d'environnements. Outre l'intégration à VMware vShield Endpoint, les utilisateurs bénéficient de la technologie unique de Bitdefender permettant de déporter des tâches, ainsi que :

- de couvrir ESXi, Xen, Hyper-V, KVM, et les autres hyperviseurs
- de s'intégrer avec vCenter et XenServer
- de protéger les postes de travail et serveurs Windows ou Linux,
- d'analyser la mémoire et les processus, en plus de la protection en temps réel du système de fichiers

Grâce à sa grande compatibilité, SVE a été la première solution de sécurité à obtenir le label Citrix Ready (http://blogs.citrix.com/2012/11/26/bitdefender-is-citrix-ready/) pour VDI-in-a-Box et d'autres solutions Citrix.

Pour plus d'informations sur GravityZone et Security for Virtual Environments, et si vous souhaitez télécharger une version d'évaluation, consultez :

- http://enterprise.bitdefender.com/fr/solutions/gravityzone/
- http://enterprise.bitdefender.com/fr/solutions/gravityzone/virtualization-security.html

1. David K Johson's post: http://blogs.forrester.com/david_johnson/13-04-01-has_vdi_peaked_a_change_in_the_adoption_drivers_sheds_new_light_and_new_life)

2. http://blogs.citrix.com/2013/07/08/top-5-scenarios-for-xendesktop-on-windows-azure/

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 500 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 Profil Technology.

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.