

# Éliminez les menaces. Pilotez les performances. Exercez un meilleur contrôle.

*Bitdefender GravityZone Security for Virtual Environments (SVE) est la solution la plus avancée du marché, qui offre une protection antimalware aux machines virtuelles et permet d'optimiser à la fois les ratios de consolidation et les coûts opérationnels. Bitdefender GravityZone SVE a été conçue pour s'adapter à la protection des plus grands datacenters, ainsi qu'aux environnements virtualisés des entreprises de toutes tailles.*

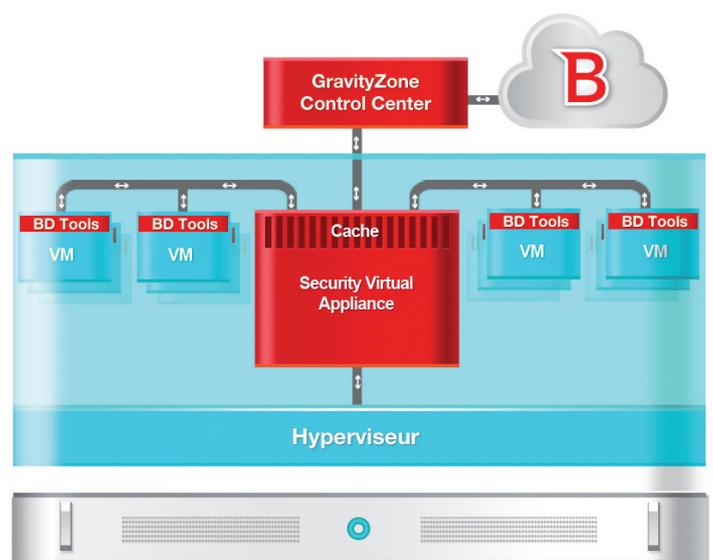
## Présentation de la technologie

Bitdefender GravityZone SVE fournit une protection antimalware via plusieurs appliances virtuelles fonctionnant en tant que serveurs de sécurité. Avec l'intégration à vShield Endpoint, il n'est pas nécessaire d'installer un agent de sécurité sur chaque VM pour assurer la protection du système de fichiers. Ce type d'agent nécessite normalement des mises à jour et une surveillance constante, et consomme des ressources locales pour fonctionner. L'agent Bitdefender Tools de chaque VM se connecte à un serveur de sécurité pour fournir une protection contre les malwares du système de fichiers. Avec l'intégration à vShield, Bitdefender étend la portée de sa protection à la mémoire, au registre et aux processus en cours d'exécution grâce à la coopération entre les VMware Tools et les Bitdefender Tools.

Bitdefender GravityZone SVE, assure également la protection des environnements qui n'utilisent pas vShield Endpoint. Dans ce cas, l'impact en termes de ressources sur les postes de travail et serveurs protégés se limite aux Bitdefender Tools. Cela fournit une protection du système de fichiers, de la mémoire, des processus et du registre à la demande aussi bien pour les VM Windows que Linux fonctionnant sous ESXi, Hyper-V, Xen, KVM, etc. En étant compatible avec tous les hyperviseurs, cette fonctionnalité permet également le basculement ("server failover") et la mobilité des serveurs de sécurité (les serveurs de sécurité sont indépendants des hôtes, ce qui est particulièrement important dans les environnements cloud publics), et offre des performances optimisées (comme le montrent les résultats des tests réalisés avec Login VSI) ainsi que d'autres avantages clés.

## AVANTAGES CLÉS

- Compatible avec VMware, Microsoft Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization (avec KVM) et d'autres plates-formes.
- Protège les machines virtuelles fonctionnant sous Microsoft et les principales distributions Linux.
- S'intègre étroitement à un nombre illimité d'instances de VMware vCenter, permettant l'interaction avec des objets tels que des pools de ressources, dossiers, réseaux distribués.
- Élimine les points de défaillance, les goulets d'étranglement et fournit une disponibilité inégalée de la protection antimalware.
- Offre la protection Bitdefender primée contre les malwares des systèmes de fichiers, de la mémoire, des processus et de la base de registre sur l'ensemble des machines virtuelles.



Bitdefender GravityZone SVE utilise un mécanisme de mise en cache multinationnel qui contribue à fournir des performances de pointe. En effet, un cache local se trouve dans chaque VM afin que les objets ne soient analysés qu'une seule fois. Ensuite, un cache partagé au niveau de chaque serveur de sécurité évite que les objets analysés sur une VM ne soient analysés sur une autre. Enfin, une série de caches au niveau des fichiers rend possible une déduplication de l'analyse sur les blocs de fichiers, ce qui signifie que les fichiers ayant peu évolué ne font pas l'objet d'une nouvelle analyse complète. L'ensemble de ces technologies exclusives de Bitdefender explique les excellentes performances obtenues par Bitdefender GravityZone SVE.

**Amazon Web Services (AWS)** – Bitdefender GravityZone SVE peut être acheté sur l'AWS Marketplace par instance et par heure. Les instances du Serveur de Sécurité et la console d'administration du Centre de Sécurité sont fournies par Bitdefender sous la forme d'un service hébergé au sein d'AWS. Pour bénéficier de la même sécurité centralisée et dédoublée que celle fournie par SVE dans les environnements privés virtualisés, il suffit de déployer les Bitdefender Tools sur les instances AWS.

L'arsenal complet des technologies de sécurité Bitdefender primées\* est intégré aux moteurs de sécurité et incorporé à l'architecture de l'appliance virtuelle. Avec Bitdefender GravityZone SVE, la protection antimalware est plus fiable que jamais et offre une haute disponibilité à chaque VM du datacenter.

## Les Bitdefender Tools en un coup d'œil

Pour que les moteurs de sécurité accèdent à chaque machine virtuelle et permettent un accès aux fichiers, à la mémoire, au registre, aux processus en cours d'exécution de la VM et aux autres fonctionnalités requises, un ensemble de services appelés les Bitdefender Tools, doivent être déployés sur chaque VM. Les caractéristiques des Bitdefender Tools sont les suivantes :

### Un impact très faible sur les ressources :

- Moins de 100 Mo d'espace lors de l'exécution (incluant le cache d'exécution).
- 15-20 Mo de mémoire locale lors de l'exécution (analyse à l'accès).
- Une charge maximale du processeur de 1-2%, sur un processeur virtuel unique pour l'analyse à l'accès.

### Caractéristiques principales :

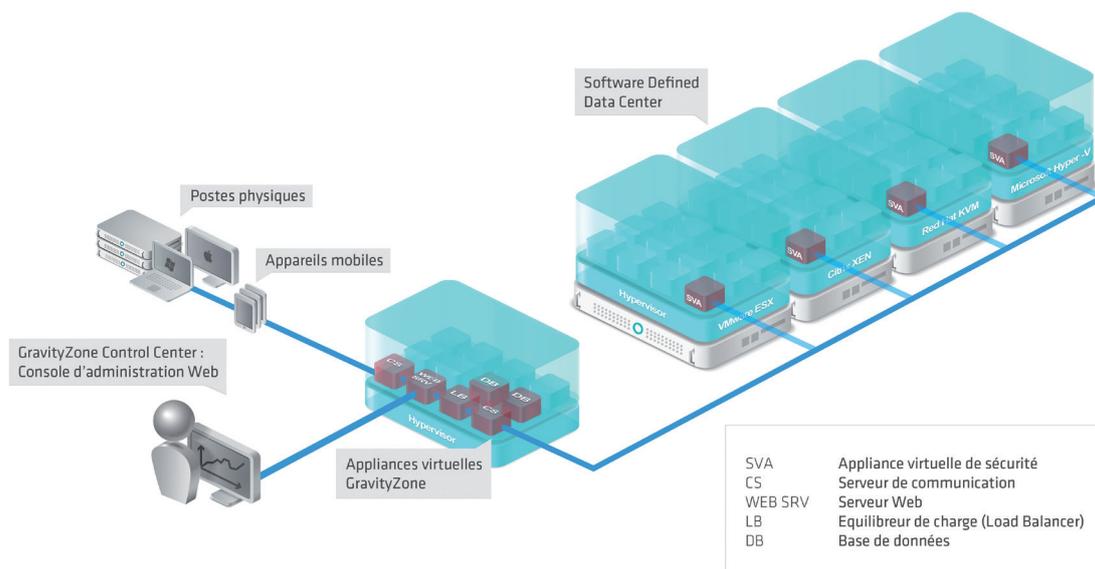
- Établissent une connexion à un serveur de sécurité autorisé disponible (une appliance virtuelle) permettant un accès local au système de fichiers, au registre, à la mémoire et aux processus.
- Se connectent à d'autres serveurs de sécurité en cas de temps de réponse trop lent ou de soudaine indisponibilité.
- Gèrent la désinfection locale, la quarantaine et le blocage des processus.
- Conservent un cache local des éléments analysés pour des gains de performances.
- S'exécutent en tant que service local sans privilèges d'administration, fournissant une protection contre les attaques tentant de désactiver la protection en local.
- Peuvent fournir une interface utilisateur à l'intérieur de la VM avec des notifications pop-up sur le bureau.
- Permettent un déploiement simple ne nécessitant pas de redémarrage.

Ils peuvent également être préinstallés dans des modèles (templates) et des images VDI sans qu'aucune maintenance ne soit nécessaire.

### Cette structure à l'architecture unique présente plusieurs avantages :

- Les machines virtuelles n'ont pas de moteurs d'analyse antivirus ni de définitions en local et sont toujours protégées lorsqu'elles sont en cours d'exécution.
- Le risque d'"AV Storms" ("conflits de ressources") est supprimé.
- La mise en cache multinationnel dans les VM individuelles et le serveur de sécurité garantit que les fichiers uniques ne sont analysés qu'une seule fois.
- Les temps de latence au démarrage sont supprimés.
- Aucun point unique de défaillance dans la protection, les Bitdefender Tools se connectant ou se reconnectant automatiquement à un moteur d'analyse disponible.
- Une protection centralisée, sans goulets d'étranglement, puisque les Bitdefender Tools peuvent passer automatiquement à un autre serveur de sécurité, disposant d'un temps de réponse plus rapide.
- Les machines virtuelles temporaires sont automatiquement protégées et la politique de sécurité prévue s'applique (lorsque les Bitdefender Tools sont installés sur l'image et que la politique de sécurité est appliquée à un dossier ou un pool de ressources).

- Une augmentation de la densité des VM, grâce à une consommation réduite de la mémoire, de l'espace disque, du processeur et du nombre d'opérations d'entrées/sorties.
- Les VM sont protégées en permanence par les dernières technologies et mises à jour, même en cas de restauration d'une ancienne image (snapshot) ou d'une sauvegarde, ou si elles redémarrent après avoir été hors-ligne pendant une longue période.



\* Les technologies brevetées comprennent B-Have, une technologie d'émulation testant les processus inconnus avant que ceux-ci ne soient autorisés à s'exécuter et Bitdefender AVC, un ensemble élaboré de méthodes d'analyse en temps réel, permettant de connaître l'activité des processus au niveau du Kernel et de l'utilisateur, comportant plus de 300 opérations heuristiques évaluant toutes les opérations au moment où elles se produisent et fournissant une protection contre les attaques de type "zero-day" et les "APT" ("Advanced Persistent Threats").

## Des performances inégalées

SVE a été conçue pour résoudre tous les problèmes liés au fonctionnement des antivirus dans un système d'exploitation virtualisé et fait l'objet d'améliorations constantes, axées sur la protection, la simplicité, les performances et la compatibilité.

Notre test de performances approfondi prouve que Bitdefender GravityZone SVE a le plus faible impact sur les performances parmi toutes les principales solutions antivirus du marché, tout en offrant un niveau élevé de protection, récompensé lors des tests indépendants. Avec Bitdefender GravityZone SVE, la densité des VM peut être augmentée de l'ordre de 30% et les coûts de fonctionnement nettement réduits grâce à une baisse drastique de la maintenance et de la surveillance.

## Un modèle de licences simple

Bitdefender GravityZone SVE propose un modèle de licences simple, par processeur ou par VM. Le modèle de licences par VM est réparti entre les serveurs virtuels et les VDI.

## Une gestion unifiée

Une licence de Bitdefender GravityZone SVE peut être obtenue via notre solution d'administration globale, GravityZone, qui est capable de gérer toutes les autres solutions : Bitdefender GravityZone Security for Endpoints, pour les ordinateurs physiques (Windows, Linux, Macintosh) et Bitdefender GravityZone Security for Mobile, pour les appareils mobiles (Android, iOS). La solution Bitdefender GravityZone repose également sur des appliances virtuelles et s'appuie sur une architecture unique basée sur des rôles permettant de s'adapter, à la demande, aux entreprises de toutes tailles en offrant un point unique de gestion centralisée de la protection. Cela permet aux clients d'accéder rapidement et facilement au déploiement, à la maintenance, à la surveillance et au reporting.

Dans un environnement mixte ou dispersé géographiquement, Bitdefender GravityZone se connectera aux datacenters quels que soient leurs emplacements et vous permettra de contrôler Bitdefender GravityZone SVE, en protégeant simultanément tous les types d'installation d'hyperviseur. L'architecture basée sur les rôles permet l'équilibrage des charges des rôles individuels afin d'éviter les goulets d'étranglement et permet de fournir un accès de qualité à l'ensemble de l'installation antivirus.

### Tester notre solution

Bitdefender GravityZone SVE est une solution antivirus inégalée que vous pourrez installer et évaluer dans votre propre environnement, en déployant des appliances virtuelles en toute simplicité. Cette installation ne demande aucune programmation puisque toute la configuration est effectuée via l'interface en ligne de l'appliance et l'interface Web intuitive de Bitdefender GravityZone. Plus de 85% des administrateurs qui ont essayé la solution Bitdefender GravityZone SVE, recommandent son achat.

**"Nous n'avons plus de problèmes de montée en charge, les appliances se déploient facilement et, une fois déployées, nous n'avons plus besoin de les surveiller, ce qui est un véritable avantage en termes de coût d'exploitation".**

Sylvain Moret, RSSI, Conseil régional de Bourgogne.

**"Nous avons donc choisi la solution Bitdefender GravityZone Security for Virtual Environments pour ses performances dans les environnements VMware et son taux de détection de virus".**

Mr Degardin (Responsable technique), La communauté d'agglomération du Pays de Grasse.

### Configuration requise et systèmes d'exploitation pris en charge

#### Systèmes d'exploitation pris en charge

OS invité

##### • Microsoft Windows

- Windows 8, 8.1 Windows 7, Windows Vista, Windows XP (SP3)
- Windows Server 2012, Windows Server 2008, Windows Server 2008 R2
- Windows Server 2003, Windows Server 2003 R2

##### • Oracle

- Solaris 11, 10

Linux

- Red Hat Enterprise 6.2, 6.1, 5.7, 5.6
- CentOS 6.5, 6.2, 6.1, 5.7, 5.6
- Ubuntu 14.04, 11.04, 10.04
- SUSE Enterprise Server 11
- OpenSUSE 12, 11
- Fedora 16, 15

#### PLATES-FORMES DE VIRTUALISATION

##### • VMware

- VMware vSphere 5.5, 5.1, 5.0 P1 ou 4.1 P3
- ESXi 4.1, 5.0, 5.1, 5.5
- VMware vCenter Server 5.5, 5.1, 5.0 ou 4.1
- VMware vShield Manager 5.5, 5.1, 5.0
- VMware vShield Endpoint
- VMware vCNS 5.5
- VMware Tools 8.6.0 build 446312
- VMware View 5.1, 5.0

##### • Citrix

- Citrix XenDesktop 7.5, 5.5, 5.0
- Citrix XenServer 6.0, 5.6 ou 5.5 incluant

##### - Citrix Xen Hypervisor

- Citrix VDI-in-a-Box 5.x
- Citrix Profile Streaming

##### • Microsoft

- Microsoft Hyper-V Server 2012, 2008 R2
- Hyperviseur Microsoft Hyper-V

##### • Linux

- Red Hat Enterprise 3.0 avec
- Hyperviseur Red Hat KVM

##### • Oracle

- Oracle VM 3.0

#### Configuration système requise

GravityZone - Security for Virtual Environments est livré sous la forme d'une appliance virtuelle Linux et est administré à partir du Control Center, une plateforme d'administration unifiée pour les postes et serveurs physiques, virtuels et mobiles.

#### Plates-Formes de virtualisation :

- VMware vSphere 5.5, 5.1, 5.0 P1 (474610-Patch#1) ou 4.1 P3 (433742-Patch#3) incluant ESXi 4.1, ESXi 5.0, ESXi 5.1, ESX 5.5 avec :
- VMware vCenter Server 5.5, 5.1, 5.0 ou 4.1
- VMware vShield Manager 5.5, 5.1, 5.0 et vCNS 5.5
- VMware vShield Endpoint installé par vShield Manager sur les hôtes
- VMware Tools 8.6.0 build 446312 installé sur les machines invitées protégées en mode complet ou avec le pilote vShield sélectionné sous VMCI, en mode personnalisé.
- VMware View 5.1, 5.0

- Citrix XenDesktop 5.5, 5.0
- XenServer 6.0, 5.6 ou 5.5 (y compris l'hyperviseur Xen)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2012, 2008 R2 ou Windows 2008 R2 (avec l'hyperviseur Hyper-V)
- Oracle VM 3.0
- Red Hat Enterprise Virtualization 3.0 (y compris l'hyperviseur KVM)
- Systèmes d'exploitation invités (32/64 bits) :
- Windows 8, Windows 7, Windows Vista, Windows XP (SP3)
- Windows Server 2012, Windows Server 2008, Windows Server 2008 R2
- Windows Server 2003, Windows Server 2003 R2
- Oracle Solaris 11, 10
- Distributions Linux :
- Red Hat Enterprise Linux 6.2, 6.1, 5.7, 5.6
- CentOS 6.2, 6.1, 5.7, 5.6
- Ubuntu 11.04, 10.04
- SUSE Linux Enterprise Server 11
- OpenSUSE 12, 11
- Fedora 16, 15

Note : Le support de la version sans agents (plate-forme VMware vShield) pour Windows 8 et Windows Server 2012 dépend de la compatibilité avec VMware vShield Endpoint et est disponible à partir de la version 5.5 de VMware vShield Manager.

Essayez Bitdefender GravityZone ! Version d'évaluation gratuite et plus d'informations disponibles sur notre site Internet :

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

Contactez notre équipe commerciale au **+33 (0)1 49 65 33 88**

Ou par e-mail : [bitdefender@profiltechnology.com](mailto:bitdefender@profiltechnology.com)

Bitdefender propose une technologie de sécurité dans plus de 100 pays via un réseau de pointe d'alliances, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.