

# Bitdefender®

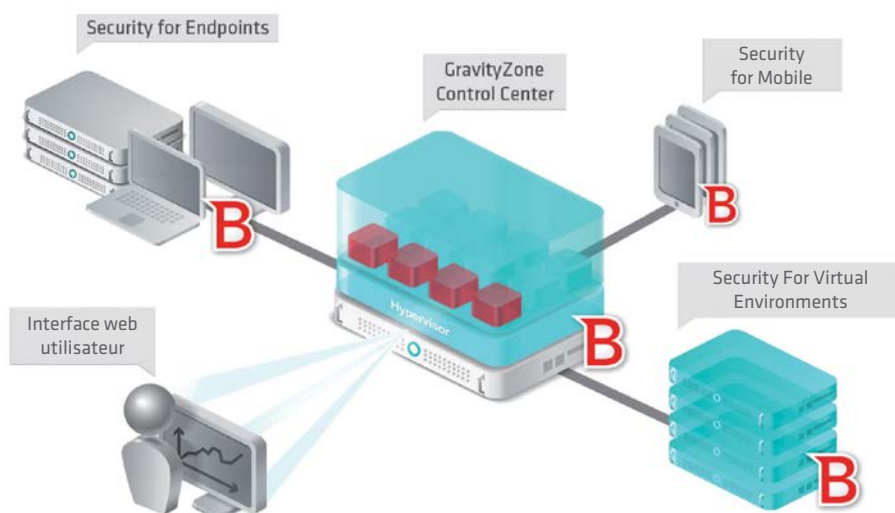
## GravityZone

### La sécurité des entreprises réinventée pour un contrôle optimisé des systèmes virtuels, physiques et mobiles

Utiliser des outils d'administration de la sécurité conçus pour les environnements d'hier oblige les services informatiques à passer trop de temps à maintenir ou contourner des solutions qui avaient été conçues pour simplifier les choses et en améliorer la gestion. La révolution entraînée par la virtualisation, le cloud computing ou le BYOD accentue le problème de la protection des environnements complexes en entreprise. Cela conduit à l'utilisation de solutions spécifiques, qui doivent être maintenues en complément de l'existant.

**Gérer la complexité avec une technologie plus intelligente :** Bitdefender GravityZone permet aux entreprises de gérer et de sécuriser les environnements hétérogènes d'aujourd'hui. La solution allie une sécurité parfaitement optimisée pour la virtualisation, à des technologies de détection de pointe en s'appuyant sur une architecture éprouvée. Elle offre aux administrateurs des fonctionnalités adaptées pour la gestion des problèmes quotidiens liés à la sécurité et supprime le besoin de recourir à des solutions spécifiques grâce à une protection unifiée, pour les systèmes virtuels, physiques et mobiles. Contrairement à d'autres solutions qui ajoutent des modules à une ancienne architecture, le tableau de bord GravityZone Control Center a été conçu spécifiquement pour unifier la surveillance et l'administration de la sécurité dans une interface unique, simple et accessible.

**Comment l'architecture fait la différence :** L'architecture unique de GravityZone lui permet d'être facilement évolutive et de protéger un nombre illimité de systèmes. Le déploiement clé en main s'effectue en important simplement une appliance virtuelle et en l'exécutant sur n'importe quelle plateforme de virtualisation. L'intégration à Microsoft Active Directory, VMware vCenter et Citrix XenServer facilite le déploiement de la protection pour les systèmes physiques et virtuels. Les entreprises peuvent ensuite déployer un ou plusieurs des services de sécurité de GravityZone : Security For Virtual Environments, Security for Endpoints et Security for Mobile. Après le déploiement initial, l'ajout de nouveaux services nécessite uniquement une activation rapide dans la console.



### AVANTAGES CLÉS

- Une sécurité conçue nativement pour réduire les problèmes liés à l'administration d'environnements complexes
- Un contrôle de la sécurité unifié pour les systèmes virtualisés, physiques et mobiles
- Une solution fournie sous forme d'une appliance virtuelle pour un déploiement simple, clé en main
- Une capacité de redondance et d'évolution prévue par défaut
- Une administration de la sécurité intégrée à Active Directory, VMware vCenter et Citrix XenServer

### PLATEFORMES DE GRAVITYZONE CONTROL CENTER

GravityZone Control Center est fourni en tant qu'appliance virtuelle et est disponible dans les formats suivants :

- OVA (compatible avec VMware vSphere, View)
- XVA (compatible avec Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatible avec Microsoft Hyper-V)

Le support d'autres formats et plateformes de virtualisation peut être fourni sur demande.

# Bitdefender®

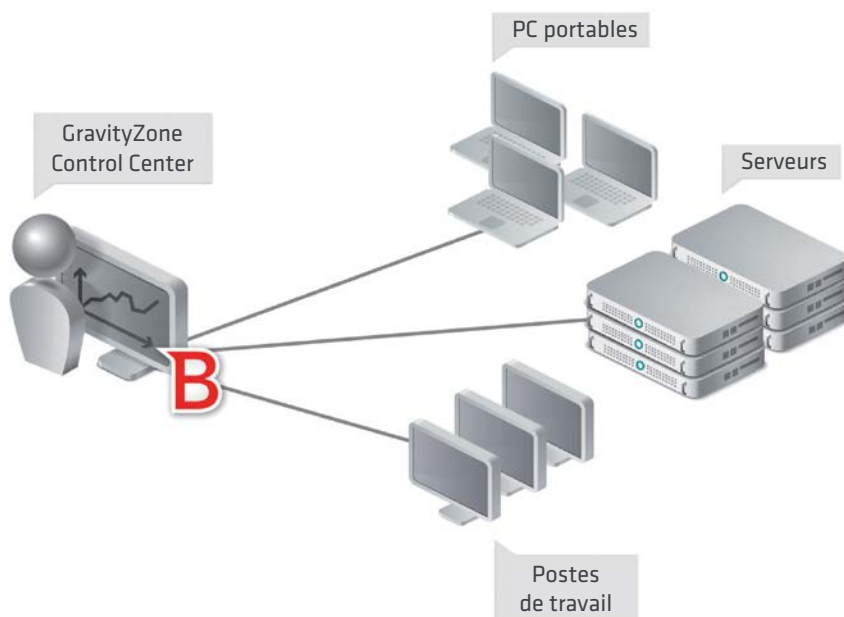
## Security for Endpoints

Security for Endpoints permet aux entreprises de déployer la protection primée pour postes de travail, ordinateurs portables et serveurs à l'aide de GravityZone, solution d'administration de la sécurité extrêmement évolutive, conçue afin de répondre aux besoins des environnements d'entreprise. GravityZone propose une sécurité éprouvée pour la virtualisation, les postes de travail physiques et les appareils mobiles et permet aux administrateurs de contrôler facilement le niveau de sécurité de leur entreprise à partir d'une seule console.

**Simplifier l'administration de la sécurité des systèmes :** Les entreprises se protègent contre des attaques de plus en plus élaborées et le poste de travail constitue la dernière ligne de défense essentielle. Cependant, la sécurité des systèmes étant parfois considérée comme une commodité, les administrateurs sont souvent obligés de se contenter de solutions traditionnelles qui, au lieu de leur fournir un contrôle de la sécurité, engendrent des problèmes et du travail supplémentaires. Security for Endpoints fournit un antimalware, un pare-feu bidirectionnel et un antiphishing, reconnus par le secteur ainsi qu'un filtrage Web et un contrôle utilisateur, administrés depuis une nouvelle console intuitive. GravityZone Control Center fournit les politiques granulaires et les données de détection en temps réel nécessaires aux administrateurs pour disposer d'une bonne vision du niveau de sécurité du réseau.

**Profiter des avantages de GravityZone à l'échelle des entreprises :** déployer la sécurité de la virtualisation GravityZone est l'occasion idéale de mettre en place une meilleure protection des systèmes et d'abandonner d'anciennes solutions laborieuses. Le service de protection des postes de travail est intégré à GravityZone et doit simplement être activé pour être effectif. Après avoir déployé un des services avec succès, la mise à niveau de la sécurité des postes s'effectue facilement et ne requiert qu'un minimum d'effort.

**Des technologies de détection constamment classées n°1 lors de tests indépendants :** Grâce à ses moteurs de signatures mais surtout à ses technologies proactives B-HAVE et Active Virus Control, Bitdefender obtient la première place lors des tests menés par AV-Test, AV-Comparatives et Virus Bulletin. B-HAVE utilise des technologies heuristiques dans un environnement virtuel (bac-à-sable) afin de repérer les menaces qui échappent à la détection par signatures alors que Bitdefender AVC est efficace même face aux techniques les plus élaborées d'évitement de détection car il surveille les processus actifs pour bloquer les comportements malveillants.



### FONCTIONNALITÉS CLÉS

- Une administration centralisée reposant sur des politiques de sécurité
- Une console de gestion, identique à celle des environnements virtualisés et des appareils mobiles
- Protection des postes physiques : ordinateurs et serveurs
- Un pare-feu bidirectionnel avec détection des intrusions
- Une protection antimalware primée
- Un antiphishing
- Un contrôle utilisateur et Web

### SYSTÈMES D'EXPLOITATION SUPPORTÉS

Security for Endpoints protège actuellement les systèmes d'exploitation suivants :

- Systèmes d'exploitation poste de travail : Windows 8, 8.1, Windows 7, Windows Vista (SP1), Windows XP (SP3),
- Mac OS X Lion (10.7), Mac OS X Mountain Lion (10.8), Mac OS X Mavericks (10.9 ou version supérieure)
- Systèmes d'exploitation tablettes et embarqués\* : Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded avec Service Pack 2, Windows XP Tablet PC Edition
- Systèmes d'exploitation serveur : Windows Server 2012, Windows Server 2012 R2, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 avec Service Pack 1, Windows Home Server

\* Pour certains systèmes d'exploitation spécifiques, des modules doivent être installés pour que Security for Endpoints fonctionne.



# Bitdefender®

## Security for Virtual Environments

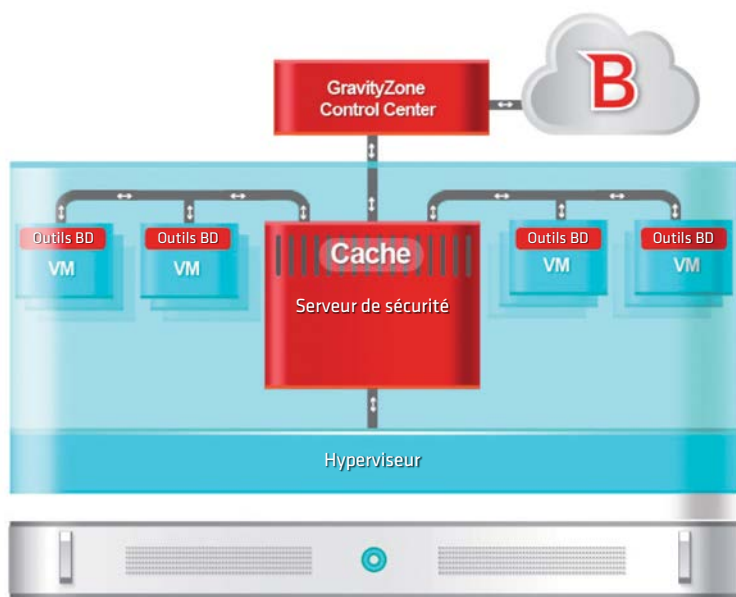
Pour la plupart des entreprises, la protection de leurs infrastructures virtualisées implique de trouver un compromis inévitable entre la sécurité et les performances. Les solutions antimalwares classiques sont souvent contre-productives puisqu'elles engendrent de nombreuses complications en matière de performance et d'administration.

Security for Virtual Environments (SVE) permet de faire face à ces problèmes avec un antimalware spécialement conçu pour protéger les serveurs et les postes de travail virtualisés sous les systèmes Windows et Linux. Contrairement aux autres solutions antimalwares, SVE n'est pas dépendante de l'hyperviseur utilisé : elle a été conçue pour fonctionner avec toutes les plateformes de virtualisation. Bitdefender fournit une appliance virtuelle dédiée permettant d'effectuer les activités antimalwares habituelles à l'extérieur des VM, ce qui offre des gains significatifs de performances et aide les administrateurs à obtenir des ratios de consolidation plus élevés.

**Des performances améliorées pour les applications :** SVE tire profit des capacités de mutualisation des ressources offertes par la virtualisation en réduisant la consommation mémoire et disque sur chaque hôte physique. Les technologies de cache dont les brevets sont en cours d'homologation, incorporées à la solution, assurent une utilisation efficace des ressources et limitent l'impact de la sécurité sur les performances des applications. SVE permet donc une augmentation des ratios de consolidation des serveurs pouvant atteindre 30% par rapport aux antimalwares classiques.

**Une configuration et une administration simplifiées :** Étroitement intégrée avec VMware vCenter et XenServer pour une administration centralisée, SVE offre d'importants avantages opérationnels allant du déploiement clé en main au reporting détaillé en passant par l'application de politiques orientées objet. Cela assure une visibilité et un contrôle complet du parc de l'entreprise et élimine les pièges habituellement liés à la sécurité traditionnelle dans les environnements virtualisés.

**Une maîtrise des coûts :** Grâce à ses technologies de pointe, de cache et d'auto-apprentissage, SVE permet la mise en place d'une sécurité ayant un faible impact sur les ressources, boostant les performances des VM et permettant une meilleure expérience utilisateur. L'amélioration de la densité du serveur engendre une baisse des dépenses de fonctionnement liées au hardware, au refroidissement et au stockage. Cela constitue un avantage de premier ordre pour tout projet de virtualisation, en entraînant un meilleur retour sur investissement et en permettant aux entreprises de tirer profit de tout le potentiel de leur investissement dans la virtualisation.



BD = Bitdefender

### FONCTIONNALITÉS CLÉS

- Une sécurité sans agent via l'intégration à VMware vShield Endpoint
- Une intégration aux plateformes d'administration VMware vCenter et Citrix XenServer
- Un support de toutes les plateformes de virtualisation : VMware, Citrix, Microsoft, Oracle, RHEV
- Une protection des systèmes de fichiers, des processus et de la mémoire sous Windows et Linux
- Une capacité d'analyse des machines virtuelles qui ne sont pas chargées (analyse hors ligne)
- Haute disponibilité à travers la répartition automatique des charges des Bitdefender Tools

### PLATEFORMES DE VIRTUALISATION SUPPORTÉES :

- VMware vSphere 5.5, 5.1, 5.0 P1 ou 4.1 P3 (y compris ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5) avec :
  - VMware vCenter Server 5.5, 5.1, 5.0 or 4.1
  - VMware vShield Manager 5.1, 5.0 and vCNS 5.5
  - VMware View 5.1, 5.0
- Citrix XenServer 6.0, 5.6, 5.5 (y compris Xen) ; XenDesktop 5.5, 5.0 ; Citrix VDI-in-a-Box 5.x
- Microsoft (Hyper-V) Server 2012, 2008 R2
- Oracle VM 3.0
- Red Hat Enterprise Virtualization 3.0 (y compris KVM)

### OS INVITÉS SUPPORTÉS (32/64 BITS) :

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



# Bitdefender®

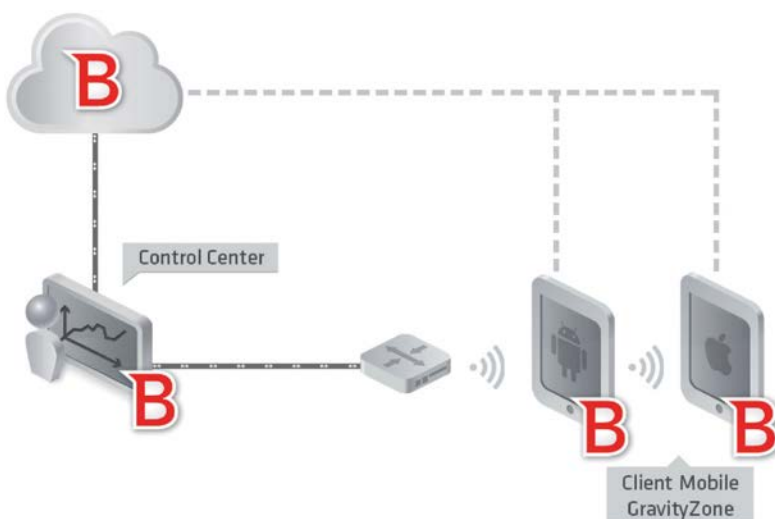
## Security for Mobile

La sécurité et le contrôle des appareils mobiles constituent un défi de plus en plus important pour les entreprises. Des volumes croissants de données d'entreprises sont accessibles à partir de ces appareils, et cela doit donc être surveillé et contrôlé. Que ces appareils portables appartiennent aux entreprises ou aux employés (phénomène du BYOD), les appareils portables contenant des données confidentielles présentent un risque potentiel s'ils ne sont pas gérés ou mal sécurisés. Si les solutions d'administration d'appareils mobiles classiques peuvent offrir des capacités de gestion des appareils dans une infrastructure mobile, elles présentent des carences en termes de sécurité et de conformité.

**Security for Mobile** introduit une approche holistique de la sécurité mobile qui aide les entreprises à assurer le respect de la conformité de leur parc tout en limitant les interventions et les tâches informatiques. En associant des toolkits d'administration simples à une sécurité mobile éprouvée, ce module de GravityZone fournit aux administrateurs les outils leur permettant d'étendre les politiques de sécurité aux appareils iOS et Android, et de protéger ceux-ci contre une utilisation non autorisée, les riskwares ou la perte de données confidentielles.

**Une visibilité et un contrôle complets :** L'intégration à Active Directory offre des avantages importants en matière de gestion, en permettant de réduire les temps d'administration et la charge de travail associée au déploiement et à l'affectation d'appareils mobiles à GravityZone. Cela élargit le périmètre de sécurité et permet aux administrateurs d'associer des appareils à des utilisateurs d'Active Directory et d'appliquer des politiques de groupes avec des actions à mettre en place sur les appareils non conformes. Ainsi, Bitdefender détecte les appareils "rootés" ou "jailbreakés" et les empêche d'accéder aux ressources de l'entreprise, en ajoutant ainsi un niveau de sécurité essentiel pour éviter la divulgation de données, en particulier en cas de perte ou de vol d'appareils.

**Une administration simple :** L'application des politiques est extrêmement simple grâce aux fonctionnalités prédéfinies telles que le verrouillage de l'écran, l'authentification, la localisation de l'appareil et le (dé)verrouillage/effacement des données à distance. Sur les appareils Android, le niveau de sécurité est amélioré avec l'analyse en temps réel et le cryptage des supports amovibles. L'administration est simplifiée avec des kits d'installation ainsi que des mises à jour délivrées via l'App Store et l'Android Market et avec un déploiement facile sur les appareils via le scan d'un QR code. Les administrateurs peuvent également gagner un temps précieux lors de la configuration initiale en appliquant à distance les paramètres réseau VPN et Wi-Fi préconfigurés via des profils.



### FONCTIONNALITÉS CLÉS

- Une obligation de verrouiller l'écran de l'appareil et d'identification.
- Le blocage de l'utilisation des appareils perdus par le verrouillage à distance
- La prévention contre la perte de données par la localisation, l'effacement ou le verrouillage à distance
- Une analyse en temps réel et un cryptage des supports amovibles pour Android.
- Une administration intégrée à MS Active Directory

### PLATEFORMES SUPPORTÉES

Security for Mobile Devices supporte les appareils mobiles et systèmes d'exploitation suivants :

- iPhones Apple et tablettes iPad (iOS 5+)
- Smartphones et tablettes Google Android (2.2+)

### À PROPOS DE BITDEFENDER

Bitdefender est une entreprise européenne qui fournit une technologie de sécurité dans plus de 200 pays via un réseau d'alliances, de partenaires distributeurs et revendeurs à valeur ajoutée. Depuis 2001, Bitdefender offre aux entreprises et aux particuliers une technologie de sécurité primée, et est l'un des principaux éditeurs de sécurité pour les technologies de virtualisation et cloud. Grâce à son département R&D, ses alliances et partenariats, Bitdefender a créé de nouveaux standards d'excellence en matière de sécurité avec ses technologies classées N°1 et ses partenariats avec des leaders mondiaux du cloud et de la virtualisation.