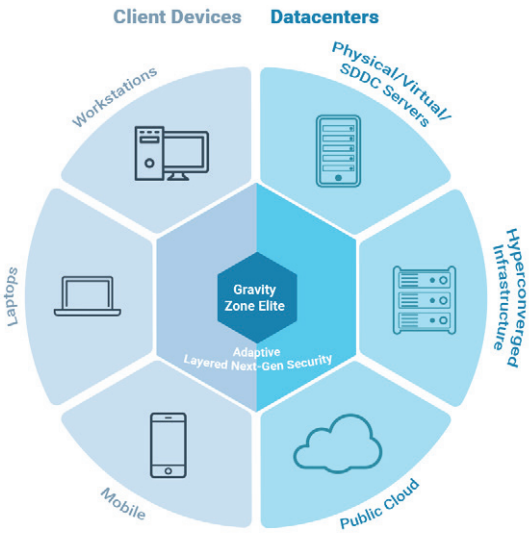
Bitdefender GravityZone Elite

Plateforme de sécurité multi-couches Next-Gen

La suite Bitdefender GravityZone Elite a été conçue pour protéger les entreprises contre l'intégralité des cybermenaces sophistiquées, et ce de manière rapide et précise. Elite combine une approche de sécurité multi-couches éprouvée de Bitdefender avec des outils et technologies Next-Gen pour assurer des performances et une protection de haut niveau pour tous les endpoints au sein de l'entreprise : ordinateurs de bureau ou portables, appareils mobiles, serveurs physiques et virtuels.

GravityZone Elite assure un niveau homogène de sécurité pour l'ensemble de l'environnement informatique, en empêchant les endpoints mal protégés de servir de point d'entrée à des actions malveillantes contre l'entreprise. Il s'appuie sur une architecture simple et intégrée avec gestion centralisée aussi bien pour des endpoints que des datacenters. Les options de console dans le cloud ou sur site sont aussi bien adaptées aux environnements cloud-ready que strictement réglementés.



POINTS CLÉS

- Détecte et bloque les attaques sans fichier
- Stoppe les attaques basées sur des scripts
- Décompresse et analyse les malwares inconnus avant leur exécution
- Un seul agent et une empreinte réduite avec un impact faible sur les systèmes
- Console d'administration intégrée pour les endpoints physiques et virtuels

Protection des endpoints

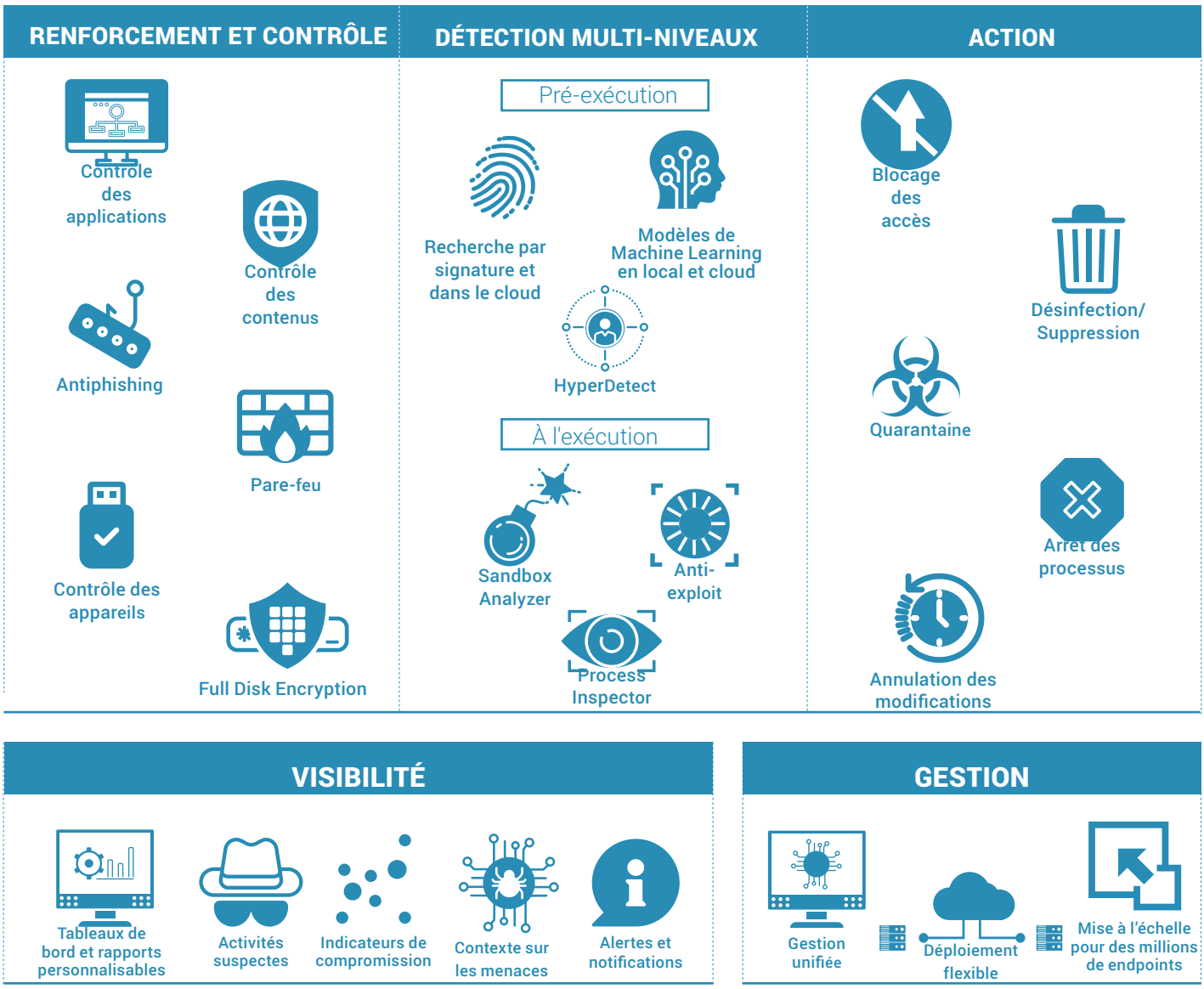
Bitdefender Endpoint Security HD – le composant de sécurité pour endpoints de GravityZone Elite - protège les entreprises contre l'ensemble des cybermenaces de manière rapide et fiable, en limitant la charge administrative et l'impact sur les systèmes. Cette solution Next-Gen élimine le besoin d'exécuter de multiples solutions de sécurité sur un même endpoint, en combinant des contrôles préventifs, des techniques de détection multi-niveaux sans signature et des réponses automatiques.

Avantages

Détecte et bloque l'ensemble des menaces sophistiquées et des malwares inconnus
Endpoint Security HD bloque les menaces avancées et les malwares inconnus, y compris les ransomwares, qui peuvent contourner les solutions traditionnelles de protection des endpoints. Les attaques avancées de type PowerShell, basées sur des scripts, les attaques sans fichier et les malwares sophistiqués peuvent être détectés et bloqués avant leur exécution.

Détecte et bloque les malwares sans fichier
Les attaques par malware sans fichier exécutent du code malveillant directement dans la mémoire. Comme aucun fichier n'est présent sur le disque, la plupart des solutions antivirus conçues pour l'analyse de fichiers ne sont pas en mesure de détecter ces attaques. Bitdefender tire profit de ses technologies Anti-exploit avancées, HyperDetect™ et de Process Inspector pour détecter, bloquer et stopper les attaques sans fichier.

Bloque les attaques basées sur des macros et des scripts
Lors de ce type d'attaque, une macro MS Office jugée fiable utilise des outils d'administration Microsoft comme PowerShell pour exécuter des scripts et télécharger du code malveillant. Comme il s'agit d'outils "fiables" de Microsoft, la plupart des produits de sécurité pour endpoints, y compris ceux dits de nouvelle génération, n'examinent pas les scripts, tels que Powershell, WMI, les interpréteurs Javascript, etc. Bitdefender intègre des techniques d'analyse des lignes de commande pour intercepter et sécuriser les scripts, avertir les administrateurs et empêcher l'exécution des scripts contenant des commandes malveillantes.



Remédiation et réponse automatiques aux menaces
Lorsqu'une menace est détectée, Bitdefender Endpoint Security HD la neutralise instantanément via des mesures incluant la fermeture des processus, la mise en quarantaine, la suppression et l'annulation des modifications malveillantes. Il partage les informations relatives aux menaces en temps réel avec Global Protective Network, le service cloud de "threat intelligence" de Bitdefender, bloquant ainsi toutes les attaques similaires dans le monde entier.

Amélioration du contexte et de la visibilité sur les menaces
La capacité unique de Bitdefender Endpoint Security HD d'identifier les activités suspectes permet d'avertir rapidement les administrateurs de comportements malveillants, tels que les requêtes douteuses faites aux systèmes d'exploitation, les mesures d'évitement et les connexions à des centres de commande et de contrôle (C&C).

Optimise l'efficacité opérationnelle grâce à un agent unique et une console intégrés
L'agent de sécurité pour endpoint, unique et intégré, limite l'impact sur les performances. Sa conception modulaire fournit un maximum de souplesse et permet aux administrateurs de définir facilement leurs politiques de sécurité. GravityZone personnalise automatiquement le package d'installation, minimisant ainsi l'impact de l'agent. Développé nativement pour le cloud et la virtualisation, GravityZone est une plateforme de gestion de sécurité unifiée de protection des environnements physiques, cloud et virtualisés.

Avantages clés

Machine Learning
Les technologies de Machine Learning utilisent des modèles et algorithmes pour prévoir et bloquer les attaques avancées. Les modèles de Machine Learning de Bitdefender utilisent 40 000 fonctionnalités statiques et dynamiques et évoluent en permanence grâce aux milliards d'échantillons de fichiers infectés ou sains, collectés auprès d'un réseau de 500 millions d'endpoints dans le monde. Une méthode qui améliore de manière spectaculaire l'efficacité de la détection des malwares, tout en limitant les faux positifs.

HyperDetect
Cette nouvelle couche de protection au niveau de la phase de pré-exécution fait appel à des modèles de Machine Learning en local et à des techniques heuristiques avancées pour identifier les outils de hacking, les exploits et les techniques de dissimulation de malwares afin de bloquer les menaces sophistiquées avant qu'elles ne s'exécutent. Elle détecte également les techniques de distribution et les sites Web qui hébergent des kits d'exploit, et bloque le trafic Web suspect. HyperDetect permet aux administrateurs d'ajuster leur protection pour contrer au mieux le type de risques auxquels

leur entreprise est susceptible de faire face. Avec l'option "Rapport uniquement", les administrateurs peuvent mettre en place et surveiller leur nouvelle politique de protection avant de la déployer, évitant ainsi les interruptions de l'activité de l'entreprise. En combinant une visibilité élevée et un blocage avancé des menaces, les utilisateurs peuvent configurer HyperDetect pour bloquer de façon normale ou permissive, tout en continuant à envoyer des rapports à un niveau agressif, pour pointer en amont les indicateurs de compromission.

Sandbox Analyzer intégré au endpoint
Cette puissante couche de protection contre les menaces avancées analyse les fichiers suspects en profondeur, exécute les charges utiles dans un environnement virtuel confiné, hébergé par Bitdefender, analyse leur comportement et réalise un rapport en cas de finalité malveillante. Intégré à l'agent endpoint GravityZone, Sandbox Analyzer envoie automatiquement les fichiers pour analyse. Lorsque Sandbox Analyzer considère un fichier comme étant malveillant, Bitdefender Endpoint Security HD le bloque automatiquement et immédiatement sur tous les systèmes de l'entreprise. La fonction de soumission automatique permet aux administrateurs de choisir entre les modes "surveillance" et "blocage", qui empêche d'accéder à un fichier jusqu'à ce qu'il ait été analysé. Les administrateurs peuvent également envoyer manuellement un fichier en analyse. Les informations complètes fournies par Sandbox Analyzer donnent un contexte clair sur les menaces et permettent de mieux comprendre le comportement de celles-ci.

Anti-exploit avancé
La technologie de prévention des exploits protège la mémoire et les applications vulnérables telles que les navigateurs Web, lecteurs de documents, fichiers médias et environnements d'exécution (Flash, Java, etc.). Des mécanismes avancés tels que la vérification de l'appelant des API, le stack pivot, le ROP (Return-Oriented Programming) et bien d'autres encore, contrôlent les routines d'accès à la mémoire pour détecter et bloquer les exploits.

Process Inspector
Process Inspector opère selon une approche "zéro confiance" pour surveiller en continu tous les processus en cours d'exécution sur le système d'exploitation. Il traque les activités suspectes ou les comportements anormaux, tels que les tentatives de dissimulation du type de processus, l'exécution de code dans l'espace d'un autre processus (détournement de l'espace mémoire pour tenter d'élever les privilèges), la réplication, le dépôt de fichiers, le camouflage face aux applications de détection des processus et bien d'autres encore. Il prend les mesures de remédiation appropriées, y compris la fermeture du processus et l'annulation des modifications réalisées par celui-ci. C'est une méthode particulièrement efficace pour détecter les malwares avancés et inconnus, ainsi que les malwares sans fichier, y compris les ransomwares.

Filtres antiphishing et de sécurité Web
Le filtrage Web analyse en temps réel le trafic Web entrant, y compris via SSL, http et https, afin d'empêcher le téléchargement de malwares sur les endpoints. La protection antiphishing bloque automatiquement les pages Web malveillantes et frauduleuses.

Full Disk Encryption
Le chiffrement de disque fourni par GravityZone se base sur Windows BitLocker et macOS FileVault afin de tirer profit des technologies intégrées au système d'exploitation. FDE est disponible en tant qu'add-on, sous licence séparée.

Contrôle des endpoints et renforcement
Le contrôle des endpoints, basé sur le système de politiques, intègre un pare-feu, le contrôle des appareils avec analyse USB et le contrôle du contenu Web avec catégorisation des URL.

Réponse et confinement
GravityZone intègre la meilleure technologie de désinfection du marché. La solution bloque/confine automatiquement les menaces, met un terme aux processus malveillants et annule les modifications réalisées.

Protection des datacenters

GravityZone Security for Virtualized Environments (SVE) tire profit de la protection multi-couches Next-Gen de GravityZone Endpoint Security HD pour assurer une sécurité de pointe aux VS, VDI et charges de travail cloud, tout en optimisant les performances de l'infrastructure et l'efficacité opérationnelle. GravityZone SVE est une solution évolutive pouvant assurer la protection des datacenters les plus complexes.

Avantages

Agilité
GravityZone SVE permet d'automatiser la sécurité tout au long du cycle de vie d'un datacenter, du déploiement aux opérations de sécurité quotidiennes d'un environnement virtuel dynamique. Il s'intègre à VMware (vCenter, vShield, NSX), Citrix XenCenter et à la plateforme cloud Nutanix Enterprise et permet un provisionnement automatisé et rapide.

Efficacité opérationnelle
La console d'administration unifiée GravityZone, le Control Center, simplifie le déploiement, la maintenance et les mises à jour de sécurité, et donne une visibilité centralisée sur tous les serveurs et postes de travail physiques comme virtuels. Il prend en charge la création centralisée et l'administration automatique des politiques de sécurité pour simplifier les opérations informatiques tout en améliorant la mise en conformité.

Meilleure utilisation de l'infrastructure
L'analyse centralisée et un agent à faible empreinte réduisent grandement l'utilisation de la mémoire, de l'espace disque, du processeur et des activités E/S sur les serveurs hôtes, améliorant ainsi la densité de VM et le retour sur investissement de l'infrastructure informatique.

Compatibilité universelle
Compatible avec toutes les plateformes de virtualisation (VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM, ou encore Nutanix® Acropolis), Microsoft Active Directory, les systèmes d'exploitation invités Windows® et Linux®, GravityZone simplifie le déploiement, la découverte des endpoints et l'administration des politiques.

Évolutivité linéaire illimitée
Plusieurs SVA peuvent être utilisées pour améliorer les capacités d'analyse lorsque le datacenter s'agrandit et que de nouvelles VM sont créées. Lorsqu'une SVA existante atteint un certain seuil de charge, de nouvelles SVA peuvent être déployées pour répondre au développement du datacenter.

Protection multi-couches Next-Gen
GravityZone SVE intègre toutes les principales couches de sécurité de Endpoint Security, dont HyperDetect, Sandbox Analyzer et les techniques de détection des attaques sans fichier, afin d'assurer une protection de pointe aux informations numériques de l'entreprise, stockées ou traitées dans le datacenter.

Sécurité pour les appareils mobiles iOS et Android

La solution est conçue pour favoriser l'adoption contrôlée du concept de "Bring your own device" (BYOD) par l'application homogène de politiques de sécurité sur l'ensemble des appareils des employés. Les appareils mobiles sont ainsi contrôlés et les informations professionnelles sensibles qui s'y trouvent sont protégées. Le contrôle de la diffusion des informations professionnelles sensibles est assuré.

Sécurité pour les serveurs Exchange

La solution intègre de nombreuses couches de sécurité pour les boites de messagerie : antispam, antiphishing, antivirus et antimalware avec analyse comportementale et assure une protection contre les menaces Zero-day ainsi qu'un filtrage du trafic, notamment des contenus et des pièces jointes. L'analyse antimalware peut être déportée vers des serveurs de sécurité centralisés depuis les serveurs de messagerie protégés. L'administration et les rapports sont centralisés, permettant ainsi l'application de politiques unifiées pour les endpoints et les boites de messagerie.

Le Control Center GravityZone

Le Control Center GravityZone est une console d'administration intégrée et centralisée qui fait office de tableau de bord unique pour toutes les composantes de gestion de la sécurité, notamment la sécurité des endpoints, des datacenters, d'Exchange et des appareils mobiles. Elle peut être hébergée dans le cloud ou déployée en local. Le Control Center regroupe de nombreux rôles et intègre un serveur de base de données, un serveur de communication, un serveur de mise à jour et une console Web. Pour les plus grandes entreprises, il peut être configuré pour utiliser de multiples appliances virtuelles avec de nombreuses instances, des rôles spécifiques et un équilibreur de charge intégré pour assurer une évolutivité importante et une disponibilité continue.

Pour consulter la configuration système détaillée, rendez-vous sur https://www.bitdefender.fr/business/elite-security.html

BD-NGZ-Oct20.2017-fr
Bitdefender-NGZ-Elite-Datasheet-creat2088-A4-fr_FR