Bitdefender

Bloque les menaces avancées et garde un coup d'avance sur les cybercriminels grâce à une sécurité pour endpoints multi-couches, adaptative

Bitdefender GravityZone Security for Endpoints bloque les menaces avancées et sophistiquées en utilisant une approche multi-couches adaptative. Nos technologies brevetées de Machine Learning combinées à la capacité à surveiller les comportements et à détecter les techniques d'attaques permettent à GravityZone de détecter et bloquer les menaces. GravityZone prend ensuite automatiquement les mesures nécessaires pour assurer la continuité de l'activité, y compris en réalisant des roll-backs lors de modifications réalisées par des malwares.

La console d'administration GravityZone centralise la gestion de la sécurité des endpoints pour les environnements physiques, virtuels et le Cloud public. Les administrateurs peuvent paramétrer précisément l'agent endpoint de GravityZone pour assurer une protection complète avec un impact minimum sur les performances.

CAS D'UTILISATION

- Blocage des ransomwares
- Protection avancée contre les menaces (protection contre les attaques ciblées avancées)
- Détection préventive des exploits - vulnérabilités Zero-day ou non corrigées
- Nettoyage - remédiation automatique
- Sécurité des datacenters
- Sécurité des environnements hybrides (Cloud public, datacenter, physique, virtuel)

AVANTAGES

Identifie et bloque les malwares et ransomwares, même inconnus
Bitdefender utilise des algorithmes brevetés de Machine Learning pour détecter avec précision les malwares inconnus, notamment les nouvelles variantes de ransomwares.
Ces algorithmes sont perfectionnés grâce à des milliards d'échantillons issus d'un réseau mondial de 500 millions de capteurs afin de prédire l'évolution des menaces et permettre à Bitdefender d'adapter ses technologies pour prendre le dessus sur les cybercriminels.

Bloque les attaques basées sur des exploits
Les attaques sophistiquées se basent souvent sur des exploits pour prendre le contrôle du poste de travail ou serveur ciblé.

La technologie anti-exploit avancée de Bitdefender détecte et bloque les attaques exploitant les vulnérabilités Zero-day et non corrigées, avec des techniques telles que le Return-oriented programming (ROP).

Détecte et bloque les attaques avancées grâce à la surveillance en temps réel
Sur le principe de « zéro confiance », la protection Bitdefender GravityZone for Endpoints surveille en permanence tous les processus actifs et peut bloquer les activités malveillantes en cours d'exécution et annuler toutes les modifications qu'elles réalisent. GravityZone Security for Endpoints peut ainsi systématiquement détecter les malwares Zero-day et les malwares sans fichier qui détournent des processus connus en cours d'exécution.

Neutralise les menaces avec remédiation automatique
Bitdefender Security for Endpoints intègre les outils de suppression des malwares les plus avancés de l'industrie afin de neutraliser instantanément les menaces, y compris les malwares les plus profondément enracinés au niveau du noyau, de supprimer tous les types de malwares, d'annuler les modifications et proposer des informations pour la remédiation et l'analyse forensics.

Performances de pointe - optimisé pour la virtualisation et le Cloud
L'agent endpoint de GravityZone est modulaire et intégré. Les administrateurs peuvent le paramétrer en fonction des fonctionnalités et politiques de sécurité nécessaires pour assurer une protection complète, avec un impact le plus faible possible sur les performances.

Visibilité et gestion de l'ensemble de l'environnement
La plateforme Bitdefender GravityZone a été conçue en partant de zéro, avec l'idée d'en faire une plateforme de gestion de la sécurité unifiée pour la protection des environnements physiques, virtualisés, Cloud et mobiles. Les rapports détaillés et la corrélation intelligente des événements fournissent des renseignements précieux sur chaque attaque, tel que le nombre de systèmes affectés, et indiquent avec précision les fichiers et exécutables impliqués.

FONCTIONNALITÉS CLÉS

Les techniques de Machine Learning utilisent des modèles et algorithmes spécialisés pour prédire et bloquer les attaques avancées avant leur exécution. Les modèles de Machine Learning de Bitdefender utilisent 40 000 fonctionnalités statiques et dynamiques et évoluent en permanence grâce aux milliards de fichiers collectés auprès de 500 millions d'endpoints protégés dans le monde. Une méthode qui améliore de manière spectaculaire la précision de la détection des malwares, tout en limitant les faux positifs.

La technologie anti-exploit avancée 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 Return-oriented programming et bien d'autres encore, contrôlent les routines d'accès à la mémoire pour détecter et bloquer les exploits.

La surveillance en temps réel des processus inspecte tous les processus du système d'exploitation en utilisant des filtres en mode utilisateur et en mode noyau. Elle traque les signes suspects ou les comportements anormaux et prend les mesures de remédiation nécessaires, notamment en terminant le processus, et annule toutes les modifications réalisées par celui-ci. C'est une méthode particulièrement efficace pour détecter les malwares avancés et inconnus ainsi que les malwares sans fichier.

Le contrôle des applications et les listes blanches* réalisent un « snapshot » de chaque endpoint et permettent aux administrateurs de créer une liste blanche des applications. Ces listes prennent en charge à la fois les modes « blocage par défaut » et « liste noire », et peuvent fonctionner en mode « Audit » ou « Renforcé ».

Le filtrage Web analyse en temps réel les e-mails entrants et le trafic Web, y compris via SSL, afin d'empêcher le téléchargement de malwares. La protection antiphishing bloque automatiquement les pages Web malveillantes.

Technologie Smart Scanning

L'analyse centralisée est disponible pour les endpoints physiques comme virtuels. Les administrateurs peuvent déporter les fonctions de sécurité, telles que l'analyse antimalware, vers une appliance virtuelle de sécurité pour préserver les ressources des endpoints. Pour les machines en itinérance, l'agent, conscient de l'environnement dans lequel l'appareil se trouve, définit la meilleure procédure d'analyse et peut décider ou non de la réaliser en local.

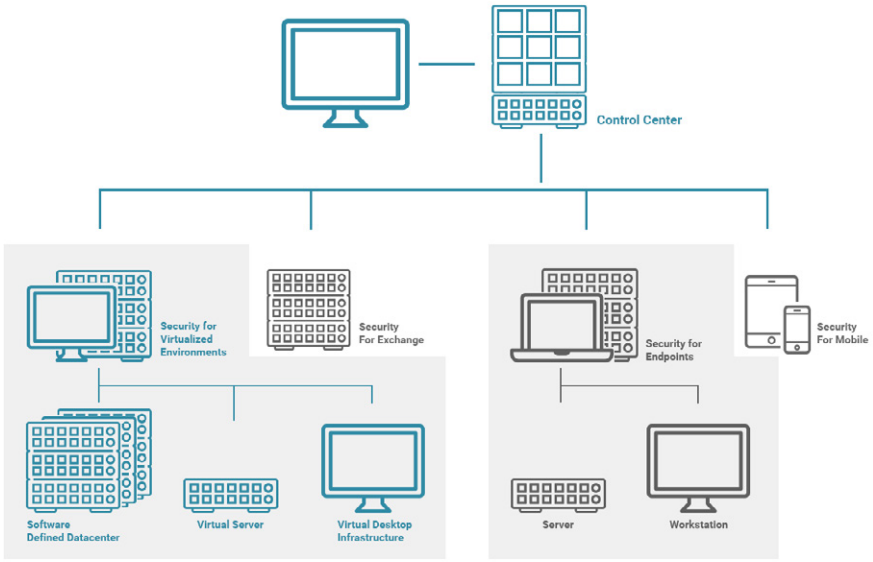
Contrôle des endpoints

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

- *Le module de contrôle des appareils* empêche l'infection par des malwares et les fuites de données en permettant aux administrateurs de gérer les permissions des appareils externes tels que les disques durs, les appareils Bluetooth, les lecteurs CD/DVD, etc.
- *Le pare-feu* intègre un pare-feu bidirectionnel et un système de détection des intrusions au niveau de l'hôte. Ce module contrôle l'accès des applications au réseau et à Internet. Il protège également le système des analyses de ports, restreint le partage de connexion à Internet et avertit lorsque que de nouveaux nœuds rejoignent une connexion Wifi.
- *Le contrôle du contenu Web* gère de manière dynamique l'accès aux sites Internet en fonction de leur contenu. La barre d'outils de Bitdefender indique aux utilisateurs la note attribuée à chaque site. La politique de contrôle Web peut bloquer l'accès au réseau d'un utilisateur ou d'une application pendant certaines plages horaires.

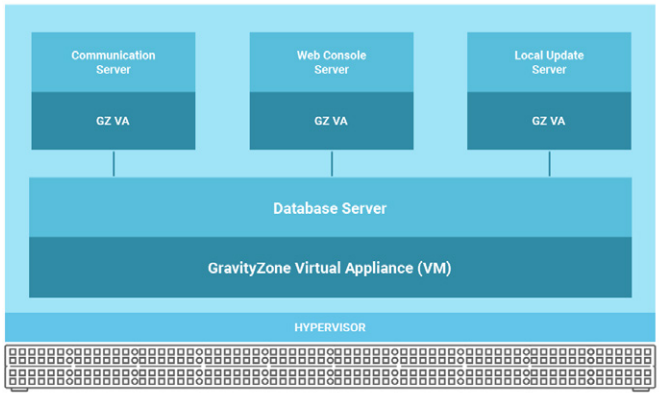
L'ARCHITECTURE BITDEFENDER GRAVITYZONE

L'architecture évolutive et résiliente de Bitdefender GravityZone comprend trois composantes clés :
• Le Control Center GravityZone
• L'agent endpoint GravityZone
• L'appliance virtuelle de sécurité (en option)



Le Control Center GravityZone
Le Control Center GravityZone est une console d'administration intégrée et centralisée pour la sécurité des endpoints, des datacenters, des boites de messagerie Exchange et des appareils mobiles.

Le Control Center GravityZone peut être hébergé dans le Cloud par Bitdefender** ou déployé sur site. Il regroupe les rôles de base de données, de serveur de communication, de serveur de mise à jour et de console Web. Il est fourni sous la forme d'une appliance virtuelle de sécurité qui peut être déployée sur site, en seulement 30 minutes. Pour les plus grandes entreprises, le Control Center GravityZone peut être configuré pour utiliser de multiples appliances virtuelles avec de nombreuses instances et des rôles spécifiques, avec un équilibreur de charge intégré pour assurer évolutivité et grande disponibilité.



L'agent endpoint GravityZone
L'agent endpoint GravityZone est composé de cinq modules :
antimalware, pare-feu, sécurité Web/contrôle de contenu, contrôle des appareils et contrôle des applications. Sa conception modulaire permet aux administrateurs de définir des politiques et services de sécurité ; GravityZone personnalise alors automatiquement le package d'installation, minimisant ainsi l'impact de l'agent sur les performances.

Pour les environnements distribués, les administrateurs peuvent tirer profit du rôle de relais et désigner des endpoints pour servir de proxy et de serveurs de mise à jour. Les agents relais détectent automatiquement les endpoints non protégés sur le réseau et déploient les packages d'installation et les mises à jour pour optimiser le trafic du réseau.

L'appliance virtuelle de sécurité
L'appliance virtuelle de sécurité est conçue pour centraliser les tâches de sécurité. La technologie Bitdefender Smart Scanning permet aux endpoints physiques et virtuels de délester leurs tâches de sécurité vers des appliances virtuelles de sécurité, libérant ainsi des ressources sur les endpoints.

* Toutes les fonctionnalités ne sont pas disponibles sur toutes les plateformes. Le contrôle des applications et les listes blanches ne sont disponibles que pour Bitdefender GravityZone Enterprise Security.

** Également connu sous la désignation de console Cloud GravityZone, disponible dans les offres Business Security et Advanced Business Security.

CONFIGURATION REQUISE ET PLATEFORMES PRISES EN CHARGE

- GravityZone Security for Endpoints et l'agent pour endpoint (appelé Bitdefender Endpoint Security Tool) sont compatibles Windows, macOS et Linux.
- Bitdefender Security for Virtualized Environment prend en charge un grand nombre d'hyperviseurs notamment, VMware ESXi, Citrix Xen, Microsoft Hyper-V, Nutanix, Red Hat KVM et Oracle VM.
- Security for Mobile Devices permet de gérer la sécurité de vos appareils Android et iOS. Pour en savoir plus sur la configuration requise, rendez-vous sur www.bitdefender.fr/business/endpoint-security.html

OPTIONS DE LICENCE

Bitdefender Security for Endpoints fait partie de la gamme de solutions Bitdefender GravityZone Business Security, Advanced Business Security et Enterprise Security. Pour obtenir plus d'informations et comparer les options des différentes offres, rendez-vous sur www.bitdefender.fr/business/compare.html

Bitdefender®

PROTÈGE PLUS DE 500 MILLIONS D'UTILISATEURS DANS LE MONDE

Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies leaders sur les marchés des entreprises et des particuliers, et est un fournisseur de choix pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à des équipes R&D, ses alliances et partenariats, Bitdefender est reconnu pour être un éditeur innovant, proposant des solutions de sécurité robustes sur lesquelles vous pouvez compter. Plus d'informations sur www.bitdefender.fr

Bitdefender®

BD-NGZ-Jun 23 2017-Tk# crea1 287
Bitdefender 2017 NGZ-EndPointSecurity-DS-crea1287-A4-fr_FR