

GravityZone Security for Containers

Protection détection et réponse pour les charges de travail natives du cloud et des conteneurs

GravityZone Security for Containers est une solution de sécurité multiplateformes très performante destinée aux conteneurs et aux environnements Linux. Elle combine un EDR à une détection avancée des exploits Linux et à une analyse approfondie des attaques.

À la différence des autres solutions, GravityZone Security for Containers intègre une pile indépendante des kernels pour Linux et les conteneurs, permettant aux entreprises d'étendre l'automatisation et la visibilité aux charges de travail cloud-natives.

Qu'est-ce qui distingue Bitdefender des autres solutions ?

- **Pile de sécurité complète conçue pour les conteneurs et les environnements Linux**—Alors que les autres produits se limitent à l'analyse des vulnérabilités ou des menaces connues et se concentrent sur les environnements Windows et les utilisateurs finaux, Bitdefender utilise une pile de sécurité conçue pour protéger les conteneurs et les hôtes Linux à l'exécution. Il identifie les exploits de type "zero-day", les anomalies et les TTP Linux, ainsi que les conteneurs qui ont été ciblés, et permet une investigation et une réponse rapides.
- **Visibilité et protection consolidées au niveau des infrastructures** – Évitez d'ajouter de nouvelles solutions ponctuelles et consolidez la sécurité avec la plateforme de sécurité des charges de travail dans le cloud, GravityZone. Elle garantit une visibilité et une protection étendues contre les menaces, couvrant les conteneurs des infrastructures IaaS et PaaS, les machines virtuelles, les utilisateurs finaux et les serveurs, les environnements Linux et Windows ainsi que les clouds privés et publics.
- **Automatisation et compatibilité étendues de la sécurité** – Préservez l'agilité du DevOps et l'efficacité opérationnelle grâce à un agent hautes performances, à un déploiement et une mise à l'échelle automatisés de la sécurité ainsi qu'à une sécurité Linux indépendante du noyau qui permet des mises à niveau vers de nouvelles distributions sans compromettre la sécurité ni créer de problèmes.

En bref

Bitdefender GravityZone Security for Containers protège les conteneurs et les charges de travail contre les attaques modernes visant Linux et les conteneurs en utilisant des techniques de prévention des menaces reposant sur l'intelligence artificielle, des technologies de lutte contre les exploits ciblant spécifiquement Linux et des systèmes de détection et de réponse sur les endpoints (EDR) tenant compte du contexte.

Avantages clés

- Visibilité et contrôle unifiés sur toutes les charges de travail, avec gestion des risques, antimalware, Machine Learning personnalisable, anti-exploit avancé et EDR avec corrélation multiplateforme.
- Efficacité de la sécurité améliorée avec une détection de 100 % des techniques d'attaques sur Linux.
- Gestion et maintenance améliorées des environnements de calculs pour diverses distributions de Linux et infrastructures de conteneurs.

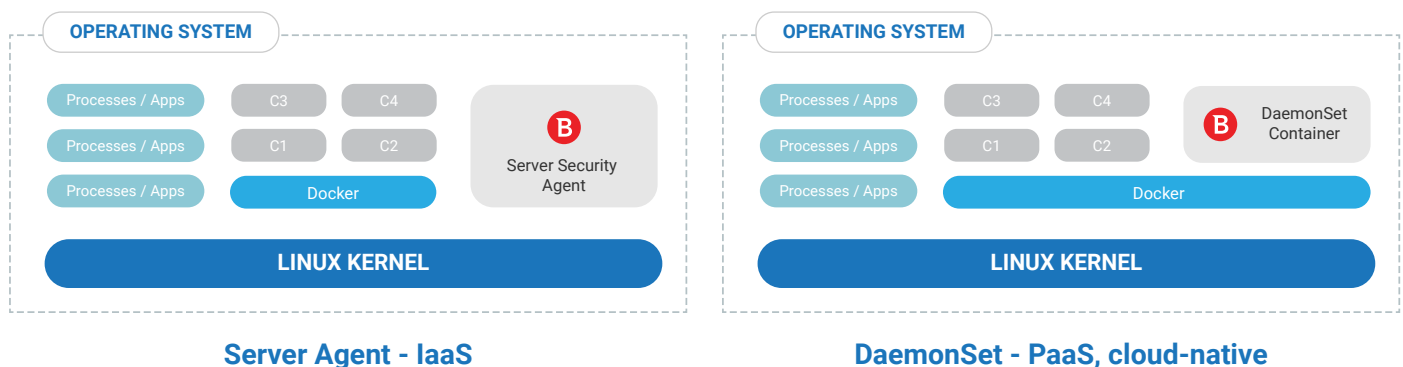
Principales capacités

- Endpoint Risk Analytics (ERA) participe à l'identification, l'évaluation et la correction des problèmes de configuration sur le conteneur hôte
- Patch Management for Linux réalise des analyses automatiques programmées pour veiller à ce que les conteneurs hôtes restent à jour
- Le Machine Learning personnalisable à l'accès (hyperdetect) détecte les attaques à haute probabilité et à fort impact tout en minimisant les faux positifs sur les menaces à plus faible risque
- Advanced Anti-Exploit bloque de manière proactive les attaques zero-day et prend en charge la plupart des exploits basés sur Linux
- L'EDR créé pour les charges de travail Linux et des conteneurs identifie les comportements suspects en temps réel tout en permettant de réaliser des audits des événements de sécurité et d'examiner en aval les attaques

Plateformes prises en charge

Infrastructures de conteneurs : Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS

Distributions Enterprise Linux : Ubuntu 16.04 LTS ou supérieur, Red Hat Enterprise Linux 7 ou supérieur, Oracle Linux 7 ou supérieur, CentOS 7 ou supérieur, SUSE Linux Enterprise Server 12 SP4 ou supérieur. Pour les autres plates-formes, consultez la page du support Bitdefender [page](#)¹.



Déploiement sous forme d'un agent invité dans votre environnement IaaS ou en tant que DaemonSet dans un environnement PaaS, cloud-native

¹ <https://www.bitdefender.com/business/support/en/77209-79472-bitdefender-endpoint-security-tools-for-linux-quick-start-guide.html>