

GravityZone Security for Containers

Kontejnery a cloudová nativní ochrana pracovní zátěže, detekce a reakce

GravityZone Security for Containers je vysoce výkonné řešení zabezpečení pro kontejnery a Linux, které je nezávislé na platformě a kombinuje rozšířenou detekci a odezvu (XDR) s pokročilou detekcí exploitů v Linuxu, a forenzní analýzou útoků.

Na rozdíl od jiných řešení obsahuje GravityZone Security for Containers stack nezávislý na jádře, vytvořený pro Linux a kontejnery, což organizacím umožňuje rozšířit možnosti automatizace a viditelnosti napříč cloudovými pracovními úlohami.

Čím se Bitdefender liší od ostatních řešení?

- **Komplexní bezpečnostní stack vytvořený pro kontejnery a Linux** - Identifikujte 1 denní exploity, anomálie a TTP v Linuxu, stejně jako cílené kontejnery, a umožněte rychlé vyšetřování a reakci pomocí bezpečnostního zásobníku, vytvořeného k ochraně kontejnerů a hostitelů Linuxu za provozu.
- **Konsolidovaná viditelnost a ochrana napříč infrastrukturami** – Vyhnete se přidávání nových jednoúčelových řešení a konsolidujte zabezpečení pomocí platformy GravityZone pro zabezpečení cloudové pracovní zátěže. Zajišťuje široký přehled o hrozbách a ochranu, která pokrývá kontejnery v infrastrukturách IaaS a PaaS, virtuální počítače, cloudové pracovní zátěže, koncové uživatele a servery, Linux a Windows, soukromé a veřejné cloudy.
- **Rozsáhlá automatizace zabezpečení a kompatibilita** – Zachovejte agilitu DevOps a provozní efektivitu, díky vysoce výkonnému agentovi, automatizovanému nasazení a škálování zabezpečení, a na jádře nezávislému zabezpečení Linuxu, které umožňuje upgrade na nové distribuce bez ztráty zabezpečení nebo vzniku problémů.

Hlavní výhody

- Analýza rizik koncových bodů (ERA) pomáhá identifikovat, vyhodnocovat a napravovat chybné konfigurace na hostiteli kontejneru.
- Rozšířená detekce a reakce (Extended Detection and Response, XDR) zajišťuje automatickou detekci a třídění výstrah na základě korelačních a detekčních algoritmů, poskytovaných jak lokálně na senzoru, tak na úrovni cloudové platformy.
- Patch Management pro Linux automaticky plánuje skenování a udržuje kontejnerového hostitele v aktuálním stavu.
- Vyladěné strojové učení na přístupu ("hyperdetect") odhaluje útoky s vysokou pravděpodobností a velkým dopadem, a minimalizuje falešně pozitivní výsledky u hrozeb s nižším rizikem.

Přehledně

GravityZone Security for Containers chrání kontejnerové pracovní zátěže před moderními útoky na Linux a kontejnery, pomocí prevence hrozeb na bázi umělé inteligence, technologií anti-exploit specifických pro Linux, a kontextově orientované detekce a reakce na koncové body s (EDR) a s XDR pro korelaci událostí napříč koncovými body, která dokáže detekovat pokročilé útoky na více koncových bodech v hybridních infrastrukturách.

Hlavní výhody

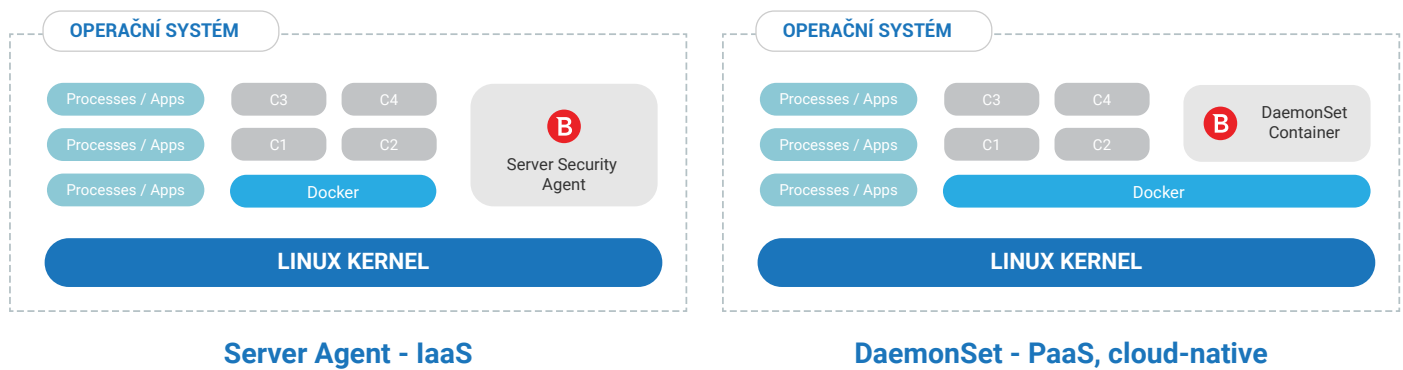
- Jednotná viditelnost a kontrola všech pracovních úloh, včetně správy rizik, antimalwaru, laditelného strojového učení, pokročilé ochrany proti zneužití, a EDR s korelací napříč koncovými body a XDR, které spojují informace o zařízeních v celé podnikové síti.
- Zvýšená účinnost zabezpečení se 100% detekcí útočných technik pro Linux.
- Izlepšení správy a údržby výpočetních prostředí v různých distribucích Linuxu a kontejnerových infrastrukturách.

- Advanced Anti-Exploit proaktivně zastavuje exploity typu zero-day, a spravuje většinu exploitů v systému Linux.

Podpora platformy

Kontejnerové infrastruktury: Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS

Enterprise Linux Distributions: Ubuntu 16.04 LTS nebo vyšší, Red Hat Enterprise Linux 7 nebo vyšší, Oracle Linux 7 nebo vyšší, CentOS 7 nebo vyšší SUSE Linux Enterprise Server 12 SP4 nebo vyšší. Další platformy naleznete na stránce [stránce](#)¹ podpory společnosti Bitdefender.



Nasazení jako Guest Agent v prostředí IaaS nebo jako DaemonSet v prostředí PaaS, cloud-native.

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