Datasheet

Bitdefender
BUILT FOR RESILIENCE

GravityZone Security for Containers

Container and cloud-native workload protection, detection and response

GravityZone Security for Containers is a platform-agnostic, high-performance security solution for containers and Linux that combines extended detection and response (XDR) with advanced Linux exploit detection, and attack forensics.

Unlike other solutions, GravityZone Security for Containers features a kernel independent stack built for Linux and containers, enabling organizations to extend automation and visibility across cloud-native workloads.

What sets Bitdefender apart from other solutions?

- **Comprehensive security stack built for containers and Linux–** Identify 0-days exploits, anomalies and Linux TTPs, as well targeted containers, and enable quick investigation and response with a security stack built to protect containers and Linux hosts at runtime.
- **Consolidated visibility and protection across infrastructures –** Avoid adding new point solutions and consolidate security with the GravityZone cloud workload security platform. It ensures broad threat visibility and protection, covering containers in IaaS and PaaS infrastructures, VMs, cloud workloads, end-user and server, Linux and Windows, private and public clouds.
- **Extensive security automation and compatibility –** Preserve DevOps agility and operational efficiency with a highly-performant agent, automated security deployment and scaling, and kernel-independent Linux security that enables upgrades to new distributions without sacrificing security or creating problems.

Key capabilities

- Endpoint Risk Analytics (ERA) helps identify, assess, and remediate misconfigurations on the container host
- Extended Detection and Response (XDR) provides automated detection and triages alerts based on correlation and detection algorithms delivered both locally to the sensor and at the cloud platform level
- Patch Management for Linux automatically schedules scanning and maintains container host up to date
- Tunable Machine Learning on access (hyperdetect) discovers high-probability and high-impact attacks, and minimizes false positives on lower-risk threats

At-a-Glance

GravityZone Security for Containers protects container workloads against modern Linux and container attacks using AI-powered threat prevention, Linux-specific anti-exploit technologies, and context-aware endpoint detection and response with (EDR) and with XDR to cross-endpoint event correlation component, capable of detecting advanced attacks across multiple endpoints in hybrid infrastructures.

Key Benefits

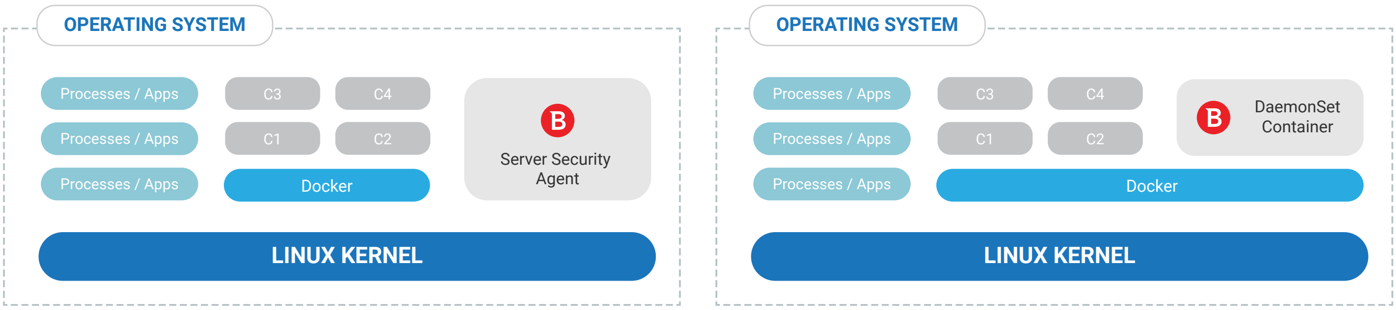
- Unified visibility and control across all workloads, including Risk Management, Antimalware, tunable machine learning, Advanced Anti-Exploit, and EDR with cross-endpoint correlation and XDR to bring together device intelligence across the enterprise network.
- Enhanced security efficacy with 100% detection of attack techniques for Linux.
- Improved management and maintenance of compute environments across diverse Linux distributions and container infrastructures.

- Advanced Anti-Exploit proactively stops zero-day exploits and manages most Linux based exploits

Platform Support

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

Enterprise Linux Distributions: Ubuntu 16.04 LTS or higher, Red Hat Enterprise Linux 7 or higher, Oracle Linux 7 or higher, CentOS 7 or higher, SUSE Linux Enterprise Server 12 SP4 or higher. For additional platforms refer to the Bitdefender support page[1].



Server Agent - IaaS | **DaemonSet - PaaS, cloud-native**

Deploy as a Guest Agent in your IaaS environment or as a DaemonSet in a PaaS, cloud-native environment

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

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

Bitdefender-BSG-GZ-SecurityForContainers-Datasheet-DEX6488-en_EN
CD-Feb/11/2022 • MD-Jun/03/2022