

## 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 endpoint detection and response (EDR) 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**—While other products are limited to scanning for known vulnerabilities or threats and concentrate on Windows and the end-user, Bitdefender uses a security stack built to protect containers and Linux hosts at runtime. It identifies 0-days exploits, anomalies and Linux TTPs, as well targeted containers, and enables quick investigation and response.
- **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
- Patch Management for Linux provides automated scheduled scanning and keeps container hosts up to date
- Tunable Machine Learning on access (hyperdetect) discovers high-probability and high-impact attacks while minimizing false positives on lower-risk threats

## At-a-Glance

Bitdefender 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 (EDR).

## Key Benefits

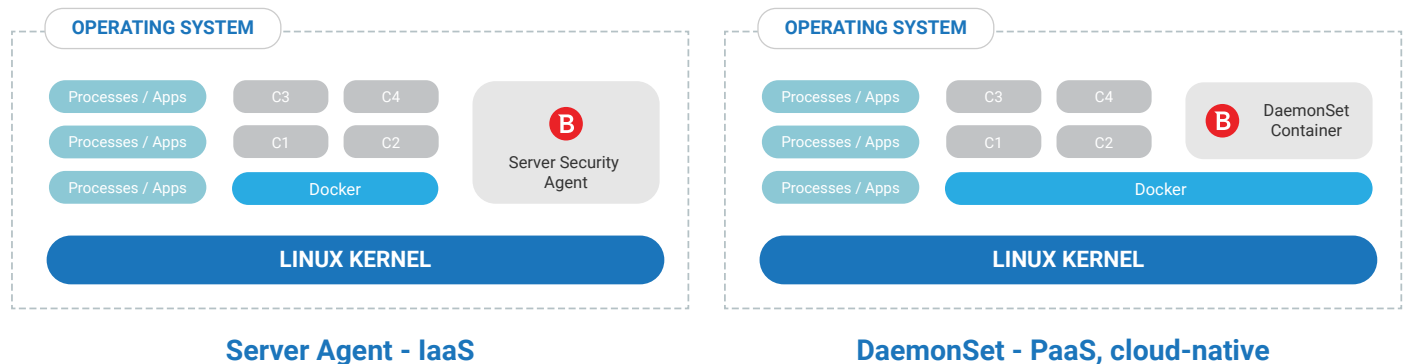
- Unified visibility and control across all workloads, including Risk Management, Antimalware, tunable machine learning, Advanced Anti-Exploit, and EDR with cross-endpoint correlation.
- Enhanced security efficacy with 100% detection of attack techniques for Linux.
- Improved management and maintenance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

- Advanced Anti-Exploit proactively stops zero-day attacks and manages most Linux-based exploits
- EDR built for Linux and container workloads flags suspicious behavior in real time while enabling security event audits and attack forensics

## 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](#)<sup>1</sup>.



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

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