

GravityZone Security for Containers

Container and cloud-native workload protection, detection and response

Bitdefender GravityZone Security for Containers is a platform-agnostic, high-performance security solution for containers and Linux that combines server extended EDR with advanced Linux exploit detection, and attack forensics.

Unlike other solutions, it features a comprehensive kernel-independent layer stack built for Linux and containers, and it enables organizations to extend automation and visibility across cloud-native workloads, VMs, containers, private, and public clouds, and physical endpoints.

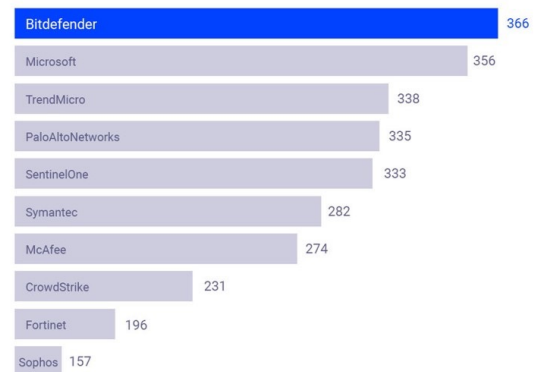
What sets Bitdefender apart from other solutions?

- **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, anomalies and Linux TTPs, as well as the containers that were targeted, and enables quick investigation and response.
- **Consolidated visibility and protection across infrastructures** – Avoid adding new point solutions and consolidate security with the Bitdefender 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 high-performance 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:

- **EDR built for Linux and container workloads** that identifies suspicious behavior in real time, enables security event audits, attack forensics and quick response actions
- **Linux Advanced Anti-Exploit** blocks Linux kernel, application zero-day and known exploit attacks
- **Platform-agnostic, high-performance security** agent ensures minimal resource impact, simplifies operations, boosts cloud ROI
- **Attacker TTPs mapped to MITRE** for Linux hones in on Linux-specific threats and displays context-rich information
- **Proven detection mastery** – Bitdefender achieved the highest total number of detections and 100% detection of attack techniques for Linux in MITRE 2021 evaluations

MITRE 2021 ATT&CK Highest Total Number of Detections and 100% Detection of Attack Techniques for Linux



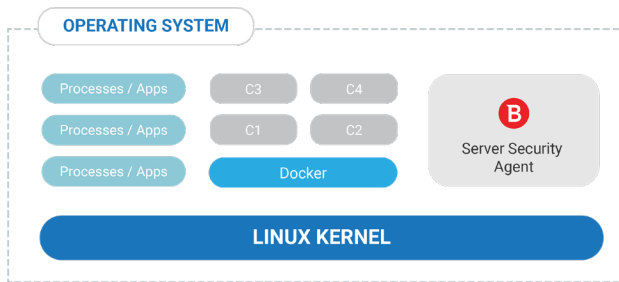
Pre-runtime image validation, immutable infrastructures and vulnerability scans are essential but do not mitigate runtime risks from 0-day threats, container escape, insider, and other attacks.

We leverage expertise into high-risk Linux server security processes via dynamic runtime analysis and dozens of proprietary machine learning algorithms to fuel unmatched advanced threat detection capabilities, which we combine with award-winning, full-stack proven prevention and detection technologies to effectively thwart malicious activity on Linux server and container workloads.

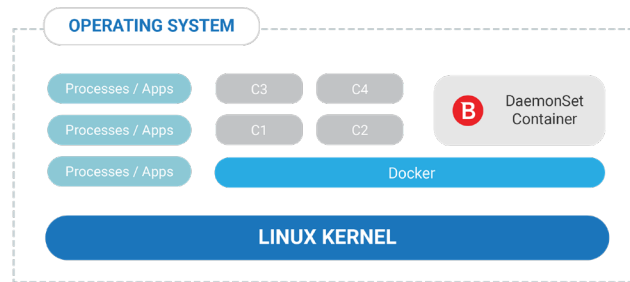
- **Container-aware incident reporting** and forensics empowers security analysts to confidently start investigating and focus the search early
- **GravityZone unified platform for CWS** ensures consolidated visibility and security control across all workloads, containers, OSs and clouds
- **Support for both IaaS and PaaS** container deployments with host agent and Daemonset deployment models
- **Comprehensive security stack** that includes Risk Management, Antimalware, Tunable machine learning prevention, Advanced Anti-Exploit and extended EDR

Platform Support

- **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, openSUSE Leap 15.2, Debian 9 or higher, Amazon Linux 2
- **Container Infrastructures:** Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS



Server Agent - IaaS



DaemonSet - PaaS, cloud-native

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne