Server Security for Linux and Containers

Purpose-Built, Multi-Distribution Security for Linux Server and Container Workloads

Bitdefender Server Security for Linux and Containers combines low-impact server workload EDR with advanced Linux exploit detection, live attack forensics, and detailed threat hunting for in-progress and historical security alerts and events. This modern attack detection and response security stack for Linux servers and containers is differentiated from existing solutions through its security efficacy, incident fidelity, and multi-distribution workload compatibility.

New security stack removes kernel dependence, allowing the upgrade of Linux kernels without fear of business interruption from security incompatibility, protecting server workloads and containerized applications/services during updates.

High-fidelity incident reporting of suspicious activity within diverse Linux and container workloads is delivered with context-rich alerts that empower SOC analysts to confidently begin investigations.

Key Differentiators

- Security stack purpose-built for diverse Linux server and container workloads
- Multi-distribution technology runs independent of Linux Kernel modules
- Superior detection and response efficacy powered by Bitdefender Labs research
- Context-aware incident reporting spans guest OS and container workloads
- Attacker TTPs mapped to MITRE ATT&CK Framework kill chain for Linux Servers

Use Cases

Secure Linux and Container Workloads

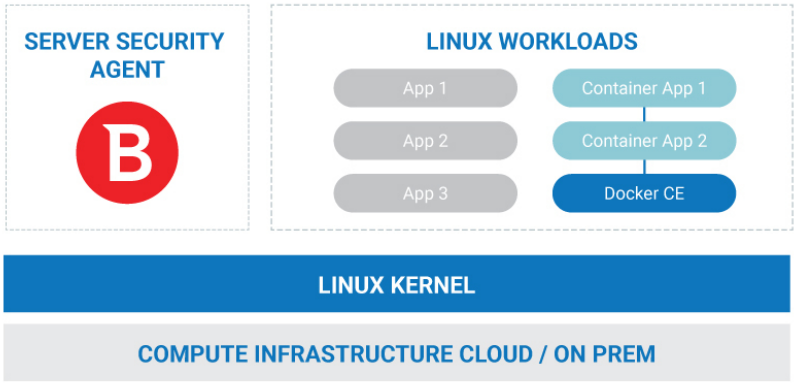
- Visibility into Linux Server and Container workload malicious activity in real time
- Understand attack risk exposure at each stage mapped to MITRE ATT&CK matrix
- Upgrade server and container infrastructure without disrupting security

Detect Advanced Exploits

- Detect complex attacks early with Linux native exploit detection technology

Incident Response

- Incident response via live query and threat hunting module



FEATURES / CAPABILITIES

- Low impact server workload EDR
- Advanced Linux exploit detection
- Platform and context-aware alerts
- Real-time attack forensics
- MITRE ATT&CK kill-chain mapping
- Live query threat hunting
- Detailed security event audit trail
- Multi-distribution Linux support
- APIs for events, assets, agent control
- Protection during OS/Application updates
- Runs alongside existing Linux security tools

PROVEN DETECTION MASTERY

Bitdefender has achieved the industry's highest efficacy out of 21 vendors on the April 2020 MITRE APT29 test with 100% ATT&CK Framework coverage

- Highest attack technique **detections**
- Highest attack technique **alerts**
- All 19 attack **kill-chain steps**

We leverage this 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.

SECURITY INDUSTRY'S #1 CHOICE

150+ VENDORS INTEGRATE BITDEFENDER TECHNOLOGIES INTO THEIR OWN PRODUCTS

38% OF CYBER SECURITY PRODUCTS WORLDWIDE USE BITDEFENDER TECHNOLOGIES

Platform Support

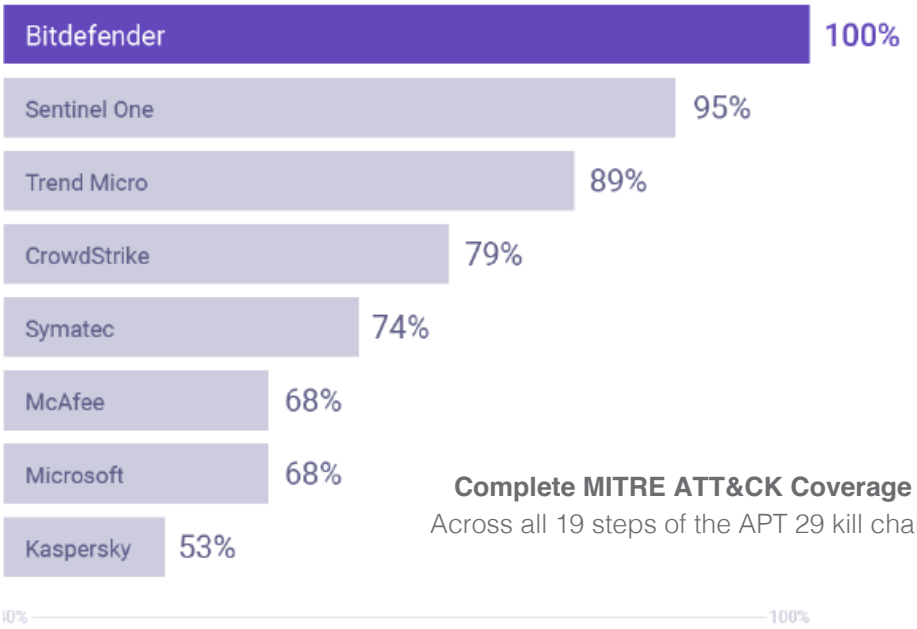
Enterprise Linux Distributions

- CentOS 7.x/8.x
- RHEL 7.x/8.x
- Debian 9 LTS
- Ubuntu 18.04 LTS / 20.04 LTS
- Oracle Linux 7.x/8.x (RHCK/UEK)
- SLES 12 SP4 and newer
- SLES 15 SP1 and newer
- Amazon Linux
- GCP Container-optimized OS

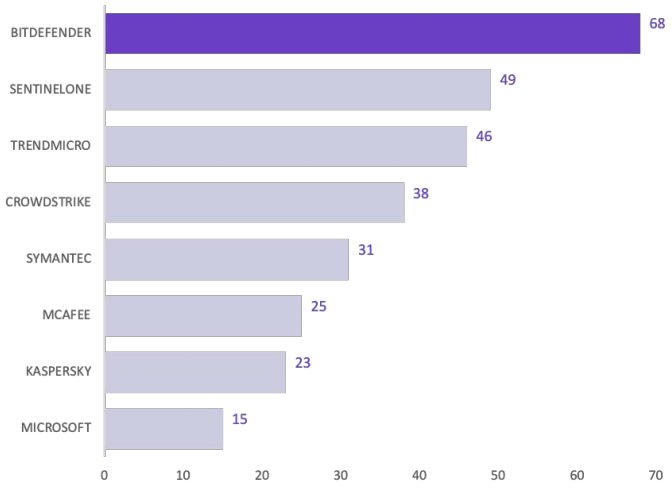
Container Environments

- Kubernetes
- Docker Container Engine

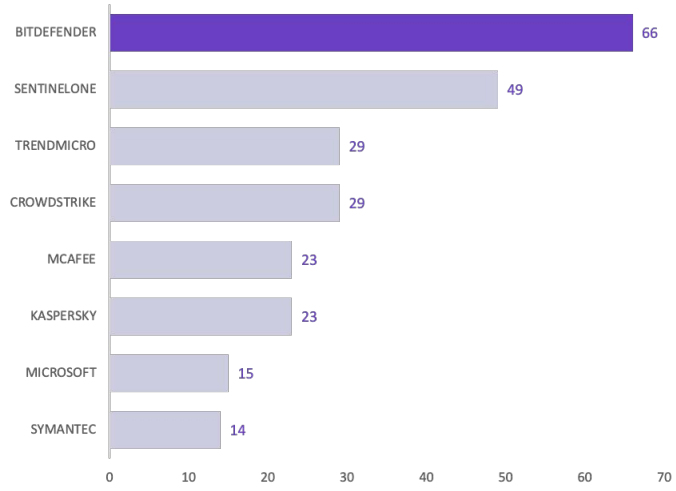
We understand the attack kill chain better than any other security vendor.
In our first MITRE ATT&CK evaluation, Bitdefender successfully completed the rigorous tests by covering all 19 attack phases against the infamous APT 29 cybercrime group.



Complete MITRE ATT&CK Coverage
Across all 19 steps of the APT 29 kill chain



Highest Number of Attack Technique Detections
across all steps in the MITRE ATT&CK evaluation



Highest Number of Attack Technique Alerts
across all steps in the MITRE ATT&CK evaluation

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