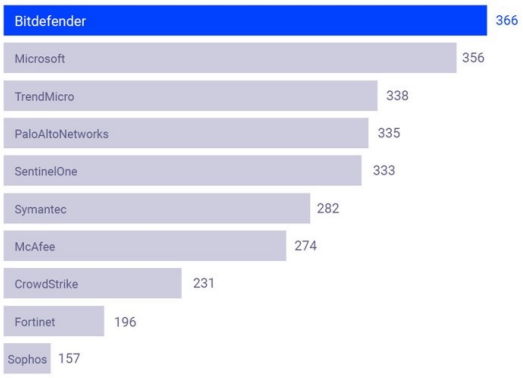
GravityZone Security for Containers

Ochrana, detekce a reakce na kontejnerovou a cloudovou zátěž

Bitdefender GravityZone Security for Containers je vysoce výkonné bezpečnostní řešení pro kontejnery a Linux, které je nezávislé na platformě a kombinuje serverovou rozšířenou EDR s pokročilou detekcí exploitů pro Linux, a forenzní analýzou útoků.

Na rozdíl od jiných řešení obsahuje komplexní zásobník vrstev nezávislých na jádře, vytvořený pro Linux a kontejnery, a umožňuje organizacím rozšířit automatizaci a viditelnost napříč cloudovými pracovními úlohami, virtuálními počítači, kontejnery, soukromými a veřejnými cloudy a fyzickými koncovými body.

MITRE 2021 ATT&CK
Nejvyšší celkový počet detekcí a 100% detekce útočných technik pro Linux



Čím se Bitdefender odlišuje od ostatních řešení?

- **Komplexní bezpečnostní balíček vytvořený pro kontejnery a Linux**—Zatímco jiné produkty se omezují na skenování známých zranitelností nebo hrozeb a soustředí se na systém Windows a koncového uživatele, Bitdefender používá bezpečnostní zásobník vytvořený k ochraně kontejnerů a hostitelů Linuxu za běhu. Identifikuje 1 - dny, anomálie a TTP pro Linux, stejně jako kontejnery, které byly cílem útoku, a umožňuje rychlé vyšetřování a reakci.
  Konsolidovaná viditelnost a ochrana napříč infrastrukturami – Vyhněte se přidávání nových bodových řešení a konsolidujte zabezpečení pomocí bezpečnostní platformy Bitdefender GravityZone pro 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.

Ověřování bitových kopií před spuštěním, nezměnitelné infrastruktury a skenování zranitelností jsou nezbytné, ale nesnižují rizika spuštění způsobená hrozbami 0-day, únikem z kontejneru, útoky zevnitř a dalšími útoky.

Využíváme odborné znalosti v oblasti vysoce rizikových procesů zabezpečení linuxových serverů prostřednictvím dynamické analýzy běhu a desítek vlastních algoritmů strojového učení, které pohánějí bezkonkurenční pokročilé schopnosti detekce hrozeb, jež kombinujeme s oceňovanými, komplexními ověřenými technologiemi prevence a detekce, abychom účinně zmařili škodlivé aktivity na linuxových serverech a kontejnerových pracovních zátěžích.

- **Rozsáhlá automatizace zabezpečení a kompatibilita –** Zachovejte agilitu DevOps a provozní efektivitu díky vysoce výkonnému agentovi, automatizovanému nasazení, škálování zabezpečení a zabezpečení Linuxu nezávislému na jádře, které umožňuje upgrade na nové distribuce bez ztráty zabezpečení nebo vzniku problémů.

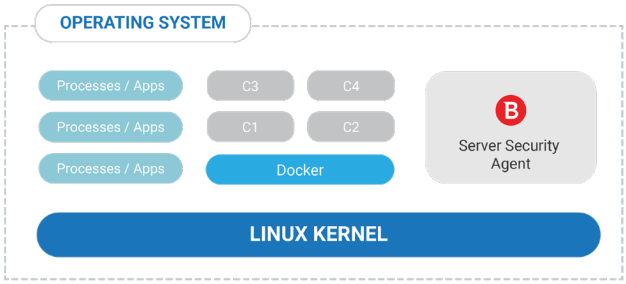
KLÍČOVÉ SCHOPNOSTI:

- **EDR vytvořená pro Linux a kontejnerové pracovní zátěže**, která identifikuje podezřelé chování v reálném čase, umožňuje audit bezpečnostních událostí, forenzní analýzu útoků a rychlou reakci.
- **Linux Advanced Anti-Exploit** blokuje útoky na jádro Linuxu, aplikace zero-day a známé exploity
- **Platformově orientovaný, vysoce výkonný bezpečnostní agent** zajišťuje minimální dopad na zdroje, zjednodušuje provoz a zvyšuje návratnost investic do cloudu.
- **TTP útočníků mapované na MITRE** pro Linux se zaměřují na hrozby specifické pro Linux a zobrazují kontextově bohaté informace.
- **Prokázané mistrovství v detekci** – Bitdefender dosáhl nejvyššího celkového počtu detekcí a 100% detekce útočných technik pro Linux v hodnoceních MITRE 2021.

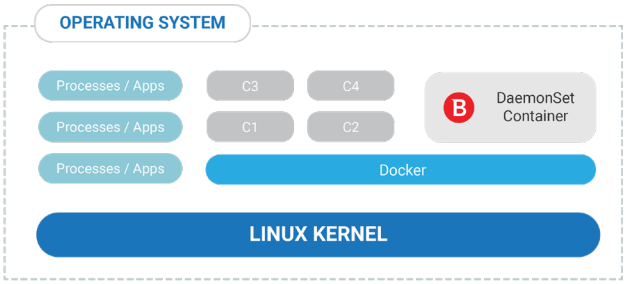
- **Hlášení incidentů a forenzní analýza s ohledem na kontejnery** umožňuje bezpečnostním analytikům s jistotou zahájit vyšetřování a včas zaměřit pátrání.
- **Jednotná platforma GravityZone pro CWS** zajišťuje konsolidovaný přehled a kontrolu zabezpečení napříč všemi pracovními úlohami, kontejnery, operačními systémy a cloudy.
- **Podpora nasazení kontejnerů IaaS i PaaS** s modely nasazení hostitelského agenta a sady Daemonset.
- **Komplexní bezpečnostní balíček**, který zahrnuje správu rizik, antimalware, vyladěnou prevenci pomocí strojového učení, pokročilý Anti-Exploit a rozšířenou EDR.

Podpora platformy

- **Distribuce Enterprise Linux**: 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, openSUSE Leap 15.2, Debian 9 nebo vyšší, Amazon Linux 2.
- **Kontejnerové infrastruktury:** Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS



Server Agent - IaaS



DaemonSet - PaaS, cloud-native

Bitdefender®

Založeno 2001, Romania
Počet zaměstnanců 1800+

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