適用於容器的GravityZone防護

容器和雲端原生工作負載的防護、偵測及回應

Bitdefender GravityZone **容器防護** 是一個適用於容器Linux之無關平台的高性能安全防護解決方案，它將伺服器擴展的EDR與進階Linux漏洞偵測和攻擊鑑識相結合。不同於其他解決方案，它具有為Linux和容器構建的核心獨立層面堆疊，且讓組織可以橫跨雲端原生工作負載、虛擬機器(VMs)、容器、 私有和公有雲端以及實體端點擴展自動化與可視性。

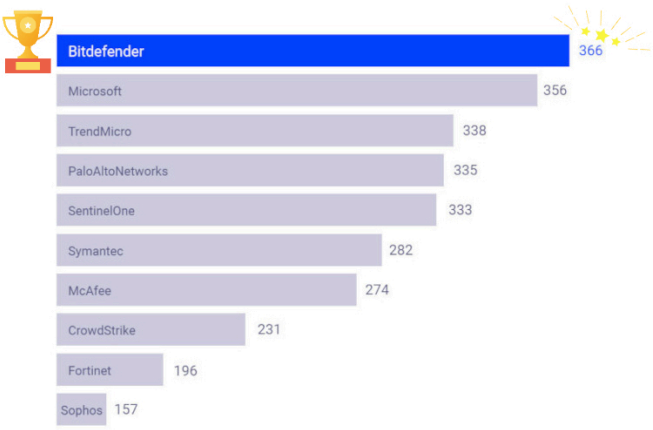
讓Bitdefender與其它解決方案不同的地方

- **為Linux和容器而構建的全方位防護堆疊**— 雖然其他產品侷限於掃描已知的漏洞或威脅並專注在Windows及終端用戶，但Bitdefender使用構建的防護堆疊在運行時保護容器及Linux主機。它可以識別零時差攻擊、異常和Linux TTPs，以及被當成目標的容器，並啟動快速調查及回應。

- **跨基礎架構的整合可視性及保護**— 避免增加新的point解決方案並透過Bitdefender GravityZone雲端工作負載防護平台鞏固安全。它確保廣泛的威脅可視性及保護，涵蓋IaaS和PaaS基礎架構、虛擬機器(VMs)、雲端工作負載、終端用戶和伺服
器、Linux和Windows、私有和公有雲端中的容器。

- **廣泛的安全防護自動化及兼容性**— 透過高性能agent，自動化安全部署與擴展保持DevOps敏捷性和運行效率，核心獨立的Linux安全防護，可以在不犧牲安全性或造成問題的情況下升級到最新的發行版本。

MITRE 2021 ATT&CK **最高總偵測數以及對Linux攻擊技術的100%偵測**



預運行時的圖形驗證、不可變的基礎架構和漏洞掃描至關重要，但不能減輕零時差威脅、容器跳脫技術、內部人員及其他攻擊帶來的運行時風險。

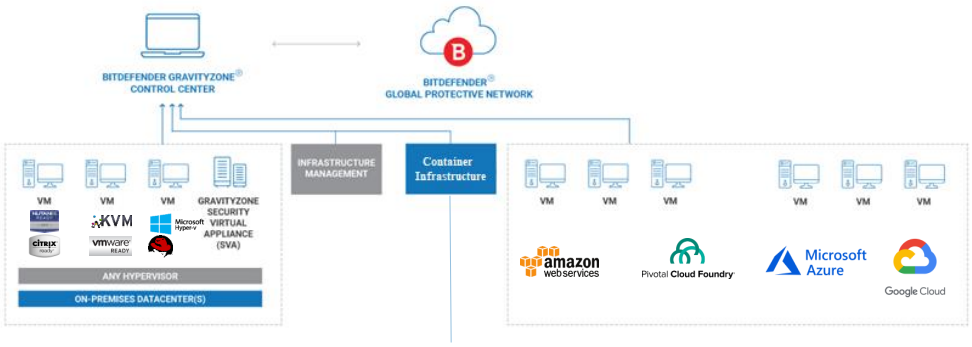
我們將專業運用於高風險的Linux伺服器安全程序，透過動態執行期分析及許多的專有機器學習演算法以推動無可匹敵的進階威脅偵測功能，我們將其與屢獲殊榮的、經全面認證的預防與偵測技術相結合，以有效阻止惡意軟體在Linux伺服器及容器工作負載上的活動。

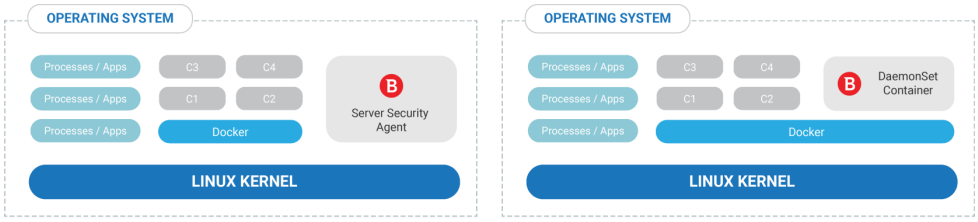
主要性能：

- **為Linux及容器工作負載而建置的EDR** 可即時找出可疑行為，啟用安全事件稽核、攻擊鑑識與快速回應行動
- **Linux進階漏洞防禦(Anti-Exploit)** 阻擋Linux核心、應用程式零時差和已知的漏洞攻擊
- **平台無關，高性能安全防護** agent確保對資源最小的影響、簡化操作、提升雲端投資報酬率
- **Attacker技術及程序(TTPs)對應至MITRE** 使Linux深入了解針對Linux的威脅且顯示內容豐富的資訊
- **認證的精湛偵測** — Bitdefender在MITRE 2021評估中實現對Linux攻擊技術最高偵測總數以及100%偵測
- **容器感知(Container-aware)事件報告** 和鑑識讓安全分析師可以自信地開始調查並盡早集中搜索
- **CWS的GravityZone統一平台** 確保跨所有工作負載、容器、OS和雲端的統一可視性及安全
- **支援IaaS與PaaS 容器部署**，透過主機agent和Daemonset部署模型
- **全方位的防護堆疊** 包含風險管理、反惡意軟體、可調式機器學習預防、進階反漏洞利用和擴展EDR

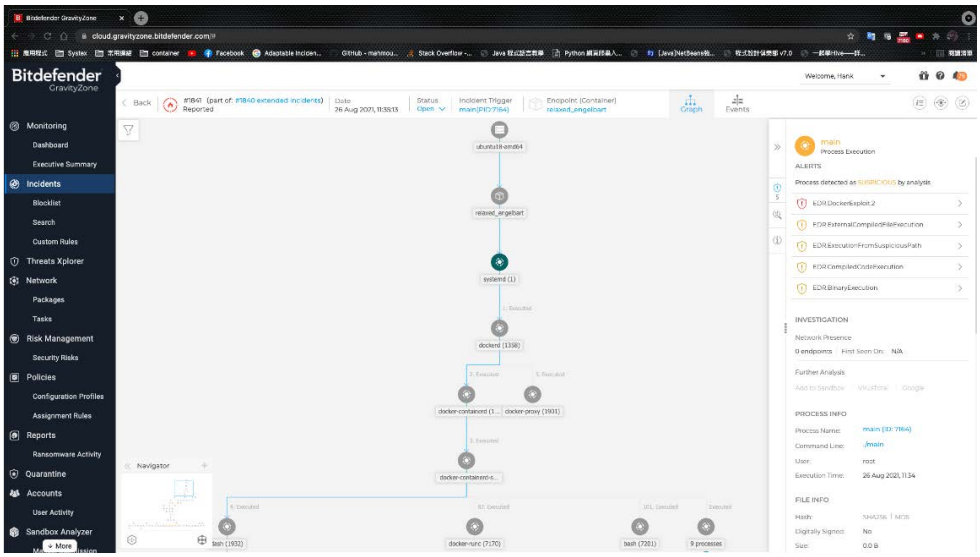
支援平台

- 企業Linux發行版本：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
- 容器基礎架構：Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS, Openshift





Server Agent - Data Center/IaaS, cloud-native　　DaemonSet - PaaS, cloud-native



完整描繪容器攻擊事件軌跡