SentinelOne

DATA SHEET

Kubernetes Sentinel Agent

SentinelOne Cloud Workload Security 模組

為容器化工作負載實現運行時保護和 EDR。

雲原生容器化工作負載如同其他運算，在運行時需要具備安全保護和端點偵測與回應 (EDR)，而 SentinelOne 提供了這些功能給 SecOps 和 DevSecOps 團隊。 Kubernetes Sentinel agents 透過對生產中容器的即時保護，來補足生產前的 CI/CD 容器掃描。運行時保護對於識別和阻止生產前掃描遺漏的以往未知的威脅至關重要。Kubernetes Sentinel 藉由啟用對容器操作 EDR 威脅搜捕的可視性，消除了 SOC 的監控盲點。

SentinelOne 為每個 node 搭配一個 agent 的一對一高效能架構，支援自我管理和託管的 Kubernetes 服務，包括 AWS EKS、Azure AKS 和 Google Cloud GKE。

Kubernetes Sentinel 的執行點與其他適用於 Windows、macOS 和 Linux 的 Sentinel，都是透過同一個多租戶控制台進行管理。藉由基於角色的存取控制，實施靈活且分散式的管理，以符合您的組織架構。Kubernetes Sentinel 為普遍被使用的 Linux 系列在維持核心模組穩定的情況下提供相容性和持續性的支援。

託管的 Kubernetes 服務

自我管理 Kubernetes

Kubernetes Sentinel 讓 SOC 透過一個簡單的 SaaS 解決方案來保護跨多個雲端服務供應商的雲原生工作負載。

KUBERNETES SENTINEL 功能

運用

+ 支援所有 Linux 主要的發行版本。
+ 無需核心模組維持作業系統穩定性。
+ 使用 Helm 封裝工具輕鬆安裝。
+ 無負擔，每個 node 搭配一個 agent，可隨著工作負載的增加和縮小自動擴展。
+ 單一控制台管理多租戶和基於角色的存取控制。
+ 針對 Kubernetes 屬性的明確標記：Clusters、Namespaces、Controllers、Pods、Containers 和 Container Images。

容器防護

+ 藉由智慧型 agent 提供沒有雲端延遲的保護。
+ 靜態 AI 功能可對 ELF、Windows 和 Mach-O 二進制檔案中的惡意軟體進行即時阻擋及隔離。
+ Behavioral AI 功能可針對以往未知的無檔案式 (Fileless) 的威脅進行即時阻止。
+ On demand 磁碟掃描。
+ 應用程式控制。

容器 ActiveEDR®

+ 專利的 Storyline 技術自動生成 PID 樹狀圖的上下關係文並重新連結。
+ 透過 Storyline 進行威脅搜捕。
+ 使用 Storyline Active Response (STAR™) 觀察可疑設備行為並做出反應。
+ 14 天 - 365 天以上的 EDR 資料保留。
+ MITRE ATT&CK 技術整合。
+ 完整性監控。

容器回應

+ 安全的遠端外殼 (RSH)。
+ 節點防火牆控制。
+ 網路隔離。
+ 文件讀取。

Storyline™ 讓 SentinelOne 成為更好的選擇

SentinelOne 獨特的專利技術 Storyline 可以減少威脅停留時間，並且讓 EDR 搜尋及搜捕操作變得更加容易。Storyline 在端點處自動地把所有軟體操作進行即時關聯，並且以秒為單位將所有流程樹狀圖上的每個過程連接，而建立可操作的上下關係文。自動回應透過 Storyline Active Response (STAR™)、XDR 雲引擎或由分析人員的手動操作在 agent 上進行即時性的觸發。

關於端點保護 (EPP)，靜態與 Behavioral AI 引擎會持續檢查數千個同時並行的作業系統狀態，找出 out-of-bounds 檔案及流程且保證做出即時的保護回應。對於端點偵測與回應 (EDR)，Sentinels 會處理困難的關聯作業，以節省分析人員的時間和煩惱。不論是惡意或良性的 Storyline 上下關係文資料，都會被長期保存在 Singularity 平台內 (14 天 到 365 天以上)，以便分析人員在必要時可立即使用。

無需再建立其他的PID 樹狀圖，由SentinelOne 為您實現。

雲原生差異

用於容器化工作負載的 Kubernetes Sentinel 提供了比其他供應商更多的即時防護、檢測、回應和可視性功能。

Kubernetes Sentinel 支援以下 LINUX 所發行的版本

- RHEL
- CentOS
- Ubuntu
- Oracle
- Amazon
- SLES Worker Nodes
- Fedora
- Debian
- Virtuozzo
- Scientific Linux

READY FOR A DEMO?

Visit the SentinelOne website for more details.

Kubernetes Sentinel 支援以下運行環境

KUBERNETES SELF-MANAGED

AWS EKS

MICROSOFT AZURE AKS

GOOGLE CLOUD PLATFORM GKE

RED HAT OPENSHIFT

創新、信賴、認可

Gartner

2021 年 Gartner 端點保護平台魔力象限的領導者

在所有關鍵能力報告案例中排名最高

MITRE ENGENUITY

刷新紀錄的 ATT&CK 評估

- 無漏失偵測，100% 可視性
- 大多數分析檢測連續運行 2 年
- 零延遲、零配置變更

Gartner peerinsights 4.9

97% of Gartner Peer Insights™

客戶評論發言推薦 SentinelOne

FedRAMP

ISO 27001 CERTIFIED by schellman

VB 100 VIRUS

TEVORA PCI DSS Attestation HIPAA Attestation

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

威雲科技 WeiCloudTech