SentinelOne

DATA SHEET

Linux Sentinel Agent

SentinelOne Cloud Workload Security 模組

在不犧牲穩定性的情況下，為本地端或雲端的 Linux 伺服器與虛擬主機，實現運行安全性和 EDR。

資安團隊對於在所有作業系統上進行防護、檢測、回應、可視性和威脅搜捕是必要的。Linux 也不例外。不同於傳統的 AV 和第一代 EDR，SentinelOne 為提升效能與自動化而建構的一個簡單 SaaS 解決方案，提供了 SOC 跨多個雲保護 Linux 所需要的進階安全功能。.

Linux Sentinel agents 是為了在資料中心或 AWS、Azure 和 Google Cloud 的實體機或虛擬機器上運行而設計的。Linux Sentinel 是安全執行點，與其他適用於 Windows、macOS 和 Kubernetes 的 Sentinel，都是透過同一個多租戶控制台進行管理。

透過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。Linux 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。

LINUX SENTINEL 差異性

- 支援各式各樣 Linux 版本。
- 無需核心模組維持作業系統穩定性。
- 對以檔案為基礎/無檔案的攻擊進行即時防禦。
- 全面性的 EDR 可視性及巨量資料的保存。
- 深度的回應能力。

運行雲原生的容器化工作負載

我們也提供以運行保護功能、EDR 功能及獨特的容器集中化為特點的 Kubernetes Sentinel 解決方案。

LINUX SENTINEL 功能

運用

+ 支援所有主要的 Linux 發行版本。
+ 無需核心模組維持作業系統穩定性。
+ 對於實體機、虛擬和雲端服務供應商可輕鬆安裝。
+ 單一控制台管理多租戶和基於角色的存取控制。
+ 應用程式目錄清單。

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。
+ 容器化工作負載用 AppCtrl。
+ 雲端虛擬機器用 AppCtrl (目前 Beta 測試階段)。

企業級 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。
+ 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。

回應功能

+ 安全的遠端外殼 (RSH)。
+ 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。**

雖然只是 Linux agent 但並不意味著功能面上有所缺乏。反之，Linux Sentinels 提供 SOC 所需要的 Linux 防護、檢測、回應和可視性等功能。

LINUX Sentinel 支援許多已發行的伺服器、VMS 和 Docker 容器，並且可以透過 ANSIBLE、CHEF、PUPPET 和 AZURE VM 擴展進行運用：

- **Ubuntu** 14.04, 16.04, 18.04, 19.04, 19.10, 20.04
- **RHEL** 6.4+, 7.1-7.8, 8.0-8.4
- **CentOS** 6.4+, 7.1-7.8, 8.0-8.4
- **Oracle** 6.9, 6.10, 7.7-7.9, 8.0-8.4
- **Amazon AMI 2**, 2017.03, 2018.03
- **SUSE Linux Enterprise Server** 12.x, 15.x
- **Fedora** 25-30, 31 kernel 5.5.x+, 32-33
- **Debian** 8, 9, 10
- **Virtuozzo** 7
- **Scientific Linux** 6, 7

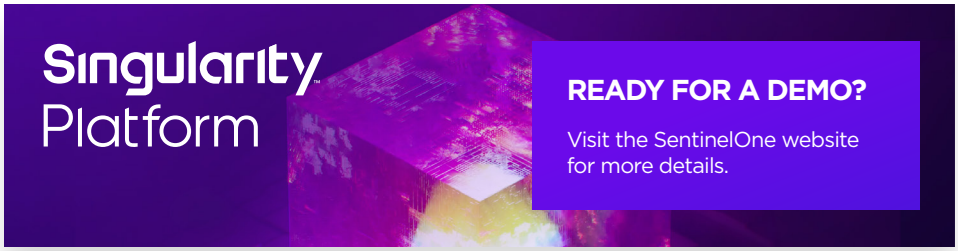
Linux Sentinel 支援以下運行環境

PHYSICAL OR VIRTUAL

AWS EC2

MICROSOFT AZURE

GOOGLE CLOUD PLATFORM



創新、信賴、認可

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

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

98% of Gartner Peer Insights™

客戶評論發言推薦 SentinelOne

FedRAMP

ISO 27001 CERTIFIED

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