SentinelOne

DATA SHEET

Singularity™ 端點保護 (EPP+EDR)

以機器速度進行自主的、AI 驅動的防護及 EDR

網路威脅的速度、複雜性和規模不斷的進化，傳統的 AV 解決方案已經無法應對。組織缺乏抵禦這些威脅所需的整體可視性和上下關係文，進而產生攻擊者可以利用的盲點。資安團隊已不堪負荷第一代 EDR 解決方案的誤報數量和低檢測效率，時常需要進行手動分類、回應和修復。

當攻擊者突破防護時，EDR 需要自主且即時的啟動。SentinelOne Singularity 端點保護 (EPP+EDR) 將次世代防護和 EDR 功能以單一 agent 形式結合在單一平台裡。

可擴充的安全性平台

Singularity 被建構成一個具有真正的多租戶和多站點層次結構的高可用性 SaaS 解決方案。SentinelOne 是端點保護領域的佼佼者，涵蓋所有主要作業系統且具有豐富的整合生態系統進而可將 Singularity 端點保護平台擴展到您既有的資安投資。

堅固的防護措施和控制

以經過訓練的靜態 AI 模組取代傳統的 AV 解決方案，藉由查看從可執行檔中擷取的各種靜態屬性來檢測威脅、消除對簽名檔的依賴性，並且對基於檔案的威脅提供卓越的檢測。透過對本機防火牆、USB、藍牙及低功耗藍牙設備的控制，來減少受攻擊面。

Storyline™ 技術進行威脅檢測

Behavioral AI 即時評估威脅 (如無檔案攻擊、橫向移動和主動執行的 rootkits 等)，在無須人工介入的情況下提供高真實度的檢測。各個事件會自動關聯到 Storyline 中並以上下關係文呈現，以便從頭到尾完整重建攻擊。來自專業和第三方來源的威脅情資，可提高檢測效率。

擁有專利的一鍵式修復

只需點擊一下即可修復所有受影響的端點，無需編寫任何新腳本，簡化流程並減少平均回應時間。使用 STAR™(Storyline Active Response) 創造符合您的環境的特定自動搜捕規則，當檢測到與規則相符之事件時，立即觸發警報並自動回應。

Deep Visibility™ 威脅搜捕

Deep Visibility 支援以零學習曲線的搜尋和調查，將資安事件回應 (IR) 和搜捕導引入更廣大的資安人才庫之中。升級 SOC 資源，藉由自動搜捕規則、情報驅動的搜捕和對 MITRE ATT&CK 技術的支援，實現主動威脅搜捕。易於使用的搜索和透視功能，可減輕分析師在對多達 365 天的大量 EDR 遙測資料進行搜索的工作負擔。

SINGULARITY EPP+EDR

以機器速度進行自主的、AI 驅動的防護及 EDR。

主要功能

+ EPP、EDR 單一或兩者結合的模組。
+ 以 AI 為基礎的惡意軟體和勒索軟體防護。
+ 無簽名檔。
+ 在線或離線的自主運行。
+ 支援 Linux、macOS、Windows、Kubernetes、Docker。
+ Storyline 自動事件相關分析。
+ 擁有專利的一鍵式修復及回滾。
+ 使用 MITRE ATT&CK 技術的搜捕。
+ STAR™ 技術進行主動、自定義搜捕和回應規則。
+ 彈性的 EDR 資料保存時間 (多達365 天以上)。
+ Singularity 平台可圓滑的融入市場。

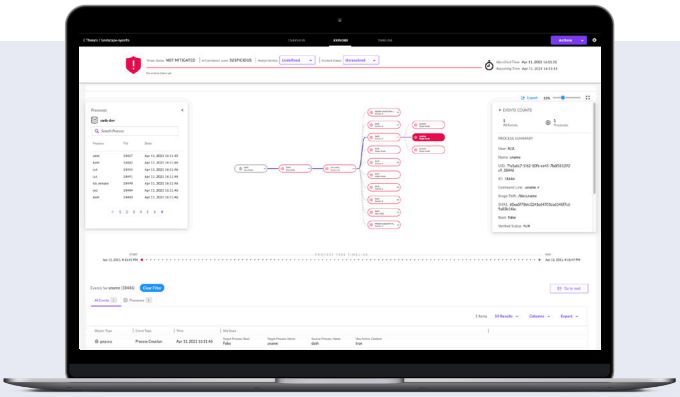
Gartner peerinsights™

“

優質的客戶服務，首選的最佳產品。

★★★★★

SENIOR DIRECTOR, IT
Healthcare



Storyline™ 自動化加速分類和搜尋

主要功能

- 滿足全球企業和託管安全服務提供商 (MSSPs) 需求的具有真正多租戶功能的單一雲交付平台。
- 無須人工介入即可自動、即時檢測和修復複雜威脅。
- 行業領先擁有最廣泛的覆蓋範圍，包括 Windows、Linux 和 macOS 的實體機、虛擬機器、雲、資料中心等任何地方。
- 一鍵式修復和回滾簡化回應流程的複雜性及減少平均修復時間 (MTTR)。
- 借助事件洞察和市場上最佳的 MITRE ATT&CK® 連結，無論是否使用 Vigilance MDR，都能加速分類和分析根本原因。利用與 Storyline 的自動關聯，在幾秒內進行調查。
- 提供 14 天 - 365 天以上的資料保存選項，可滿足各種需求。
- 快速部署的互操作性功能，確保快速、順利展開。
- 從領先級的第三方和專業來源取得用於檢測和豐富內容的整合式威脅情資。

優點

+ 更短的滯留時間
+ 迅速的事件回應時間
+ 減少平均修復時間 (MTTR)
+ 減少誤判導致的警報疲勞
+ 整體可視性
+ 分析師生產力提升
+ 最少的管理與維護成本

READY FOR A DEMO?

Visit the SentinelOne website for more details

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 ★★★★★

98% of Gartner Peer Insights™

客戶評論發言推薦 SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · 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