SentinelOne

DATA SHEET

SentinelOne 端點防護平台

SentinelOne Singularity™ 產品介紹

SentinelOne 資訊安全管理平台賦予 SOC 及 IT 團隊更有效率的方式應對日益複雜的資安威脅並保障企業資訊安全。

SentinelOne 針對端點防護、端點事件偵測與回應、IoT 設備防護、雲端防護及 IT 團隊的運作提供不同的解決方案 - 將多種技術整合至統一的管理平台，SentinelOne 針對 Windows、Mac、Linux 及 Kubernetes 提供高效率的 Agents 並且能針對客戶不同環境架構，包含實體環境、虛擬環境、VDI、客戶數據中心、混合式數據中心及雲端服務供應商.....等各種環境進行佈署。

SentinelOne Agents 透過全球各地提供的 SaaS 雲端平台統一進行管理，直覺化操作介面及彈性化管理方式可滿足企業的各式需求。SentinelOne 所提供的 Vigilance Managed Detection & Response (MDR) 訂閱式服務更可確保企業能夠得到 24x7 不間斷的支援服務。

本文件提供 SentinelOne 產品不同層級的訂閱項目 - Singularity Core、Control 及 Complete。每一層級的產品皆向下包含前一層級功能。

為何選擇 SentinelOne？

- SentinelOne 透過完整整合 EPP 及EDR 產品消除冗贅產品重複安裝佈署的資源消耗。
- 97% 客戶支援滿意度。
- 97% 客戶推薦 SentinelOne。
- 省時、高效率且可調整內容的管理平台。
- 進階動態行為 AI 偵測引擎可有效阻擋勒索軟體。
- 自動化事件處理、立即解決威脅事件。
- 專利技術 Storyline™ 透過 ActiveEDR® 為事件處理及威脅獵捕提供完整攻擊流。
- 可加值將 EDR 資料保留期增加至 365 天+ 完整保存歷史資料。
- 可快速與其他產品進行 XDR 整合。

Singularity 管理平台功能與特色

SentinelOne SaaS 雲端管理平台針對所有訂閱層級提供以下功能：

- 全球性 SaaS 平台建置、高可用性、可選擇地區包含：US、EU、APAC。
- 針對管理者登入與授權機制彈性調整，可選用機制包含：SSO、MFA、RBAC。
- 管理者權限控制可針對客戶個別需求進行調整。
- 365 日威脅事件資料保留期。
- 高度整合 SentinelOne 威脅情資與 MITRE ATT&CK 威脅指標。
- 數據化 Dashboard 針對威脅事件提供數據量化。
- 針對不同情境調整通知，並可選擇透過 Email 或 Syslog 發送。
- Singularity Marketplace 生態鏈提供多項不同產品與一鍵整合 Apps。
- API 整合式介面提供超過 340 種以上功能。

Singularity Core

Core License 為 SentinelOne 提供的端點防護產品的最核心功能。針對尋求次世代端點防護軟體以取代現有傳統防毒軟體或無效軟體的客戶，Singularity Core 提供更有效率且更簡易管理的端點防護軟體 (EPP)。 Core License 提供的基礎 EDR 功能更可讓客戶體驗完整 EPP 與 EDR 整合產品的防護能力。
SentinelOne 所提供的威脅情資透過端點防護的 AI 偵測功能及 SentinelOne 雲端情資將給予客戶以下功能：

- **內建 AI 靜態偵測引擎及 AI 動態行為偵測引擎** 預防並即時偵測各種可能的攻擊或威脅，在造成任何傷害前進行阻擋及防禦。Singularity Core 針對已知或未知的威脅具有絕佳的防禦能力，包含惡意程式、木馬、駭客程式、勒索軟體 、記憶體漏洞、惡意腳本及巨集.....等。
- **Agent 自動化事件處理** 無論是否有網路連線，SentinelOne 皆能針對惡意程式或攻擊事件即時進行偵測及阻擋。
- **快速復原** 讓使用者能夠在數分鐘之內快速復原系統，無須重新建置或撰寫複雜腳本，在攻擊或事件發生期間任何未經授權的系統變更皆可透過管理平台一鍵進行緩解 (Remediation) 或在 Windows 作業系統上完成一鍵還原 (Rollback)。
- **高度安全 SaaS 雲端管理平台存取權限** 客戶可選擇透過 US、EU或 APAC 地區存取管理平台。根據不同站點或群組建立數據化的 Dashboards、防護規則修改、整合 MITRE ATT&CK 的惡意事件分析.....等功能。

Singularity Control

Control License 除了包含 Core License 的功能外，更額外針對端點安全性及軟硬體控管提供額外相關功能。
Control License 包含所有 Core License 功能並額外提供客戶以下功能：

- **防火牆控管** 針對進出端點的網路連線行為與方向進行控管。
- **裝置控管** 針對 USB 裝置、藍牙裝置及藍牙相關裝置進行存取權限控管。
- **Rogue 裝置掃描** 可掃描網域位置中尚未安裝 SentinelOne 的裝置。
- **應用程式弱點管理** 除了可提供端點安裝軟體清單外，更針對安裝的第三方軟體整合 MITRE CVE 資料庫提供該軟體已知的弱點清單及詳細資料。

SENTINELONE STOPS RANSOMWARE AND OTHER FILELESS ATTACKS WITH BEHAVIORAL AI AND STRONG AUTOMATIC REMEDIATION FUNCTIONS

Singularity Complete

Complete License 提供客戶包含端點防護、端點安全性控管及 SentinelOne 的進階 EDR 功能 (ActiveEDR®) 。 Complete License 所提供的專利 Storyline™ 技術能將端點系統的處理程序 (包含重新啟動前後的相關處理程序) 完整進行實時紀錄、儲存並自動進行關聯，提供客戶日後進行調查。 Storyline™ 可免除資安團隊進行事件分析時所耗費的大量時間並快速提供事件相關資訊。 Singularity Complete 透過將事件自動化進行關聯並且整合至 MITRE ATT&CK®框架降低資安人員、SOC 分析團隊、威脅獵捕人員和事件處理人員的工作壓力，即便是持有最高標準及需求的國際企業也選擇使用 Singularity Complete 來滿足其資安需求。 **Complete License 包含所有 Core 及 Control License 並額外提供客戶以下功能：**

- **專利 Storyline™ 技術** 快速對事件進行根本原因分析 (RCA) 及事件重點關聯。
- **整合 ActiveEDR® 可見性** 整合所有正常資料及威脅事件資料。
- **資料保留期限可調整** 從 14 到 365+ 日以上皆可根據企業需求調整。
- **透過 MITRE ATT&CK® 技術進行威脅獵捕。**
- **管理者可手動將 Storyline™ 資料標記為威脅** 並透過端點防護對其進行處理。
- **透過 Storyline Active Response (STAR™)** 為客戶量身打造客製化事件處理方式。
- 攻擊事件時間示圖、遠端連線 Remote Shell、取得威脅檔案、第三方 Marketplace 應用程式沙箱整合.....等其他功能。

Gartner peerinsights™

“

Impressive capabilities. Easy to deploy and use EDR.

Director of Cybersecurity - Heathcare
1B - 3B USD

Gartner peerinsights™

“

Single platform the SOC can rely on.

Security & Risk Management - Finance
50M - 250M USD

IT Central Station
Unbiased reviews from the tech community

“

Increased efficiency. We've absolutely seen an ROI.

Global InfoSec Director - Manufacturing
10B - 25B USD

Vigilance Response MDR 訂閱式服務

SentinelOne Vigilance Response 以及 Response Pro Managed Detection & Response (MDR) 訂閱式服務是專為 SentinelOne 的端點方戶軟體為強化客戶資訊安全所提供的額外服務。Vigilance MDR 透過檢視、處理、紀錄並根據情況會報所有威脅事件最大化提升SentinelOne 產品效益及價值。

在大多數情況下，SentinelOne 專業分析團隊將會在威脅事件發生的 20 分鐘內針對該事件進行分析、處理並針對重要與緊急事件進行通知，確保使用者掌握站內資訊安全。

Vigilance MDR 為 SentinelOne 重要的加值服務項目，讓客戶能專注於真正重要的事件並降低企業內部 IT / SOC 團隊龐大的工作壓力。

更多資訊請參閱：
www.sentinelone.com/global-services/services-overview/

SentinelOne Readiness 訂閱式服務

SentinelOne Readiness 為協助 SentinelOne 進行大量佈署前的準備階段、佈署中以及佈署建置完成後提供建議與協助的諮詢式服務，讓客戶能夠快速且有效率地完成 SentinelOne 產品佈署並確保其隨著時間的推進能夠順暢運行。

Readiness 訂閱式服務能夠確保客戶以最務實的計畫進行產品佈署與安裝，並提供定期的升級支援服務。此外，Readiness 訂閱式服務提供每季一次的 ONEscore™ 健全性檢測以確保客戶客戶環境架構中的 SentinelOne 產品隨時處於最佳狀態。

更多資訊請參閱：
www.sentinelone.com/global-services/readiness/

各層級訂閱項目功能

	Singularity Complete	Singularity Control	Singularity Core
全球 SaaS 管理平台權限、存取權限控管、高可用性、各層級防護規則設定、EDR 事件處理分析與主動式威脅獵捕、IoT 裝置控管 (包含 Ranger 相關功能)、雲端安全服務	✓	✓	✓
資訊安全營運與 EDR 功能			
Deep Visibility ActiveEDR® 完整事件呈現	✓		
MITRE ATT&CK® 整合	✓		
STAR自定義偵測規則	✓		
STAR Pro自定義偵測規則	+		
即時惡意程式資料庫	+		
檔案合規性監控	✓		
EDR搜索資料14天保留期	✓		
EDR搜索資料保留期最高可提高至365天	+		
雲端資料庫存取備份	+		
Remote Shell	✓	✓	
IT 營運 / 端點控管套件相關功能			
OS 防火牆控制與進出點紀錄 (Win、Mac、Linux)	✓	✓	
USB 裝置控管 (Win、Mac)	✓	✓	
藍牙與 BLE® 裝置控管 (Win、Mac)	✓	✓	
未安裝 SentinelOne 裝置查詢	✓	✓	
應用程式風險偵測 (Win、Mac)	✓	✓	
端點防護相關功能			
專利技術 Storyline™ 自動化事件關聯	✓	✓	✓
靜態 AI 偵測 & SentinelOne 雲端資安情資資料庫	✓	✓	✓
動態行為 AI 偵測無檔案惡意攻擊	✓	✓	✓
自動化事件處理 Kill, Quarantine (Win、Mac、Linux)	✓	✓	✓
自動化威脅事件緩解 One-click Remediation Response (Win、Mac)	✓	✓	✓
自動化系統自動還原 One-click Rollback Response (Win)	✓	✓	✓
受感染裝置斷網功能	✓	✓	✓
事件分析功能 (MITRE ATT&CK®、事件時間圖、攻擊示圖、團隊分析標記)	✓	✓	✓
SentinelOne Agent 防竄改保護機制	✓	✓	✓
端點安裝軟體清單	✓	✓	✓

額外項目

	Singularity Complete	Singularity Control	Singularity Core
Singularity RANGER			
Ranger 網路資產管理	+	+	
Ranger 網路攻擊控制	+	+	
Agent 自動化佈署 (即將推出)	+	+	
獵捕特定裝置潛在威脅	+		
Singularity Cloud			
Kubernetes and VMs 雲端防護	+	+	+
雲端服務 Metadata 整合	+	+	+
Kubernetes 自動化 Apps 控管	+	+	
Linux VMs 自動化 Apps 控管	+		
工作負載 CIS 安全配置指引 (CIS Benchmark™)整合 (即將推出)	+		

全球支援與服務

電話、網路及 Email 技術支援服務	**訂閱已包含**
管理平台資源中心 / Support Portal 存取權限	**訂閱已包含**
標準 9x5 技術支援	**訂閱已包含**
企業級 24 小時全年無休技術支援、針對事件層級 1 ~ 2 提供 24 小時服務	可額外選購
企業級支援 + 技術支援經理	可額外選購
Vigilance Respond - 託管式偵測及回應	可額外選購
Vigilance Respond Pro – MDR服務 +安全事件分析	可額外選購
SentinelOne Readiness – 佈署與更新支援	可額外選購

SENTINELONE LOCATIONS

Mountain View, CA (HQ)
Tel Aviv, Boston, Amsterdam,
Tokyo, Oregon US

GLOBAL DATA CENTERS

US, Frankfurt, Tokyo,
AWS GovCloud

Highly Available