SentinelOne

資料表

SentinelOne 端點安全產品

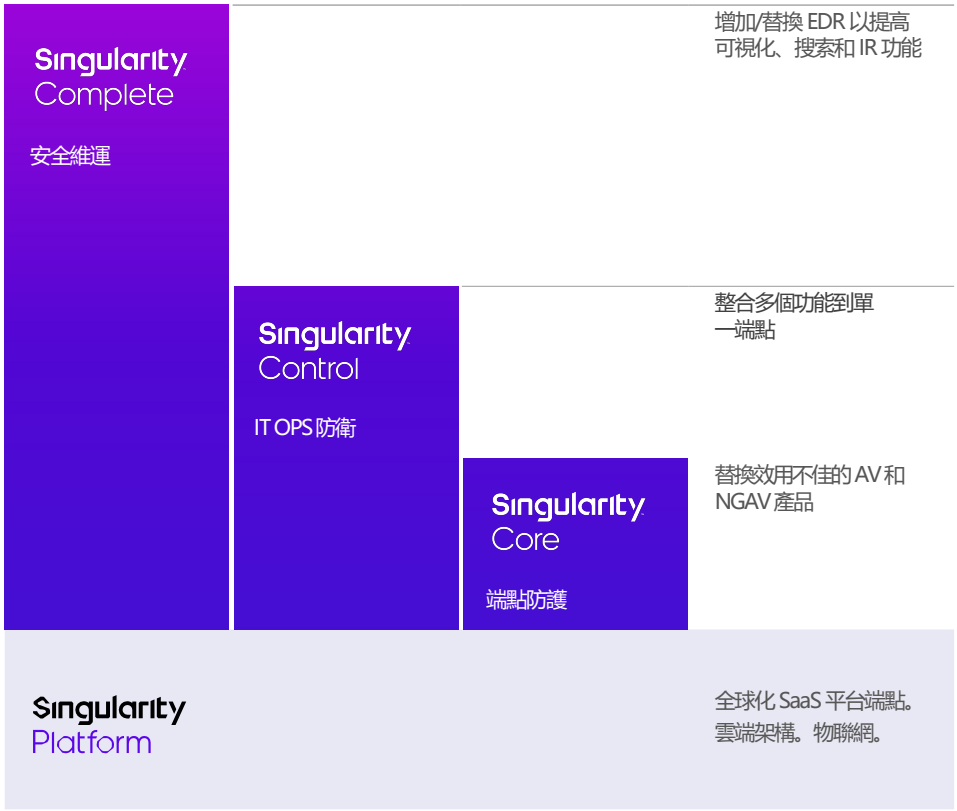
Singularity™ Platform 產品線

SentinelOne Singularity Platform 為 SOC 和 IT 維運團隊提供了一種更有效的方式來保護資訊資產不會受到當今複雜威脅的危害。

Singularity 提供差異化的端點保護、端點威脅偵測應變、物聯網安全、雲端安全和 IT 維運能力 —— 將多種現有技術整合到一個解決方案中。我們為 Windows、Mac、Linux 和 Kubernetes 提供使用極少資源的 Sentinel 代理程式，並支援實體機、虛擬機、VDI、本地資料中心、混合雲資料中心和雲服務提供商等各種形式及架構。

Sentinel 透過我們全球都可連上的多租戶 SaaS 環境進行管理，設計上也能滿足您要求的容易上手和靈活管理。我們的 Vigilance Managed Detection & Response (MDR) 訂閱服務可 24x7 全天候為您的組織安全提供技術支援。

此資料表描述了產品線內 Singularity Core、Control 和 Complete 各個產品的差異。每個產品的功能描述都在下面的產品套裝組合表格內提供。



為什麼選擇 SENTINELONE?

- 我們的端點安全的確極為出色。SentinelOne 真正結合了 EPP+EDR，讓您減少了多餘的端點代理程式，以及降低人力管理所需的OPEX成本.
- 97% 的客戶技術支援滿意度
- 97% 的客戶推薦 SentinelOne
- 具備可節省工作流程時間的客製化控制台
- 透過出色的 Behavioral AI 解決勒索軟體問題
- 快速觸發自主保護應變
- 具備使用 Storyline™ 技術且為事件應變處理者和威脅獵補者而專門設計的 ActiveEDR® ，可節省時間、減少過高的人力分析.
- 經濟實惠的 EDR 資料可保留 365 天以上，以供完整的歷史數據分析（*選購）
- 輕鬆與其他供應商的 XDR 整合

需要現場展示嗎?

請參觀 SentinelOne 網站並觀看更多細節

Singularity Platform 功能與產品

所有 SentinelOne 用戶都可以存取這些 SaaS 管理控制台功能:

- 全球 SaaS 部署。高可用性。在地化地點選擇（美國、歐盟、亞太地區）。
- 靈活的管理認證和授權：SSO、MFA、RBAC
- 管理可客製化以相容於您的組織架構
- 365 天威脅事件儲存
- 整合 SentinelOne 威脅智慧和 MITRE ATT&CK 威脅指標
- 數據驅動的儀表板安全分析
- 可設定為透過電子郵件和Syslog通報
- Singularity Marketplace 生態系統，包含bite-sized, 1-click APP
- 可利用單一 API 整合超過 340 多個功能

Singularity Core

Core 具有 SentinelOne 端點安全產品線的基本核心功能。它是我們的入門級端點安全產品，適合於希望用更有效且更易於管理的 EPP 取代傳統 AV 或 NGAV 的組織。 Core 還提供基本的 EDR 功能，展示了 EPP+EDR 功能的真正結合。威脅情報是我們標準產品的一部分，並透過我們的 AI 功能和 SentinelOne Cloud 進行整合。Singularity Core 功能包含了:

- **內建 Static AI 及 Behavioral AI 分析：** 在造成損害之前即時預防和檢測各種攻擊。 Core 可防禦已知和未知的惡意軟體、特洛伊木馬、駭客工具、勒索軟體、記憶體漏洞、腳本濫用、惡意巨集等。
- **Sentinels 可自行作用的：** 這表示在無論有沒有與雲端建立連接的情況下都可以應用預防和檢測技術，並即時觸發防護回應。
- **恢復速度極為迅速：** 讓用戶在幾分鐘內恢復工作，無需重新安裝和編寫腳本。攻擊期間發生的任何未經授權的更改都可以透過 Windows 的 1-Click Remediation 和 1-Click Rollback 回復。
- **安全的存取 SaaS 管理介面：** 可根據所在地自行選擇美國、歐盟、亞太地區。數據驅動的儀表板、按站點和群組進行安全政策管理、與 MITRE ATT&CK 的事件整合分析等等。

Singularity Control

Control 是專為在 Singularity Core 中尋求進階功能的組織而設計．可透過加選適用於端點管理的"安全擴充套件" 來達到最佳安全性． **Control 包括所有 Core 具有的功能以及**:

- **防火牆控制：** 用於設備內的網路連接控制，包括位置感知
- **設備控制：** 用於 USB 設備和藍牙/低能耗藍牙 等周邊設備控制
- **惡意設備可視化：** 使網路上需要 Sentinel 代理程式保護的設備無所遁形
- **弱點管理：** 除了應用程式資產清單之外，還可以深入了解具有對應到 MITRE CVE 資料庫的第三方應用程式已知漏洞

Sentinelone 透過Behavioral AI 和強大的自動修復功能阻止勒索軟體和其他無檔案病毒攻擊

Singularity Complete

Complete 專為需要新世代端點保護和控制以及我們稱為 ActiveEDR® 的進階 EDR 功能的企業而設計。 Complete 還擁有獲得專利的 Storyline™ 技術，可以無時無刻自動將所有作業系統程序關係（甚至在重新啟動之後）情景化，並將它們儲存起來以供將來調查使用。 Storyline™ 使分析師不再將時間用於事件關聯工作，並讓他們快速找到根本原因。 Singularity Complete 主要功能在透過自動關聯後自動傳導並將其對應到 MITRE ATT&CK® 框架來減輕安全管理員、SOC 分析師、威脅獵捕者和威脅事件回應者的負擔。最挑剔的全球化企業客戶運行 Singularity Complete 是為了滿足他們絕不屈服的網路安全需求。 Complete 包括所有 Core 和 Control 的功能以及：

- **專利 Storyline™** 用於快速根因分析和簡單的樞紐表
- **整合 ActiveEDR® 可視化：**來處理良性和惡意數據
- **滿足您所需要的數據保留天數選項：** 最少14天，最多365天以上
- **使用 MITRE ATT&CK ® 技術進行誘捕**
- **標示良性 Storylines 為威脅** 由 EPP 功能強制執行
- 自定義檢測和自動搜索規則 **Storyline Active Response (STAR™)**
- 時間軸、remote shell、檔案取得、沙箱整合等

Gartner peerinsights™

“

令人印象深刻的能力。易於部署和使用的 EDR.

網路安全總監 – 健康照護產業
1B - 3B USD

Gartner peerinsights™

“

SOC 可依賴的單一平台.

安全與風險管理部門 - 財務金融業
50M - 250M USD

IT Central Station
Unbiased reviews from the tech community

“

明顯提昇效率。我們明確的看見了ROI

全球信息安全總監 - 製造業
10B - 25B USD

Vigilance MDR 服務訂閱

SentinelOne Vigilance Managed Detection & Response (MDR) 是一種訂閱服務，旨在增強客戶安全組織。 Vigilance MDR 透過確保對每個威脅進行審查、處理、記錄和根據需要升級來增加價值。在大多數情況下，我們會在大約 20 分鐘內解釋和解決威脅，並且只會在緊急情況下與您聯繫。 Vigilance MDR 使客戶可以只關注於重要的事件，使其成為適合人力資源緊張的 IT/SOC 團隊的完美端點附加解決方案。

更多資訊請點擊下列連結：
www.sentinelone.com/global-services/services-overview/

SentinelOne Readiness 服務訂閱

SentinelOne Readiness 是一項諮詢訂閱服務，旨在透過結構化的方法在產品安裝之前、安裝中以及安裝後指導您的團隊，讓您快速啟動和運行順暢，並隨著時間的推移使您的安裝保持健康狀態。Readiness 客戶透過部署最佳實務得到指導，提供定期代理程式升級技術支援，並可接受每個季度的 ONEscore 健康檢查，以確保您的 SentinelOne 資產得到優化。

更多資訊請點擊下列連結：
www.sentinelone.com/global-services/readiness/

套裝產品功能比較

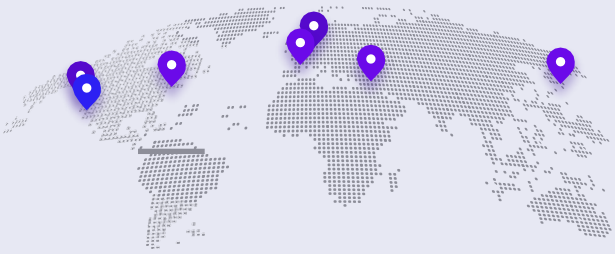
	Singularity Complete	Singularity Control	Singularity Core
全球 SaaS 平台. 安全存取, 高可用性, 階層式安全政策管理, EDR 事件應變與威脅誘捕, 分析, IoT 控制（可加選 Ranger), CWS	✓	✓	✓
資訊安全功能 EDR 功能			
使用 Storyline™ 前後文技術的 ActiveEDR® 深度可視化	✓		
MITRE Engenuity ATT&CK® 整合	✓		
Storyline Active Response (STAR™) 客製化偵測安全規則	✓		
Storyline Active Response (STAR) Pro 客製化偵測安全規則	+		
Binary Vault 即時惡意軟體上傳儲存庫	+		
文件完整性監控	✓		
EDR 獵捕數據保留 14 天	✓		
延長 EDR 獵捕數據保留 日數至365 天	+		
Cloud Funnel™ 資料湖串流	+		
Secure Remote Shell	✓	✓	
IT OPS / Security Hygiene & Suite Features			
具有位置偵測功能的 OS 防火牆控制 (Win, Mac, Linux)	✓	✓	
USB 設備控管 (Win, Mac)	✓	✓	
藍芽/低功耗藍牙 周邊設備控管 (Win, Mac)	✓	✓	
App 弱點 (Win, Mac)	✓	✓	
惡意設備掃描功能	✓	✓	✓
端點防護基本功能			
使用 Storyline™ 引擎的自主化 Sentinel 代理程式	✓	✓	✓
Static AI 與 SentinelOne Cloud Intelligence 基於檔案的攻擊防禦	✓	✓	✓
Behavioral AI 無文件攻擊檢測	✓	✓	✓
Autonomous Threat Response / 中止, 隔離 (Win, Mac, Linux)	✓	✓	✓
Autonomous Remediation Response / 一鍵完成, 無劇本編寫 (Win, Mac)	✓	✓	✓
Autonomous Rollback Response / 一鍵完成, 無劇本編寫 (Win)	✓	✓	✓
將設備從網路隔離	✓	✓	✓
事件分析 (MITRE ATT&CK®, 時間線、瀏覽、團隊註釋)	✓	✓	✓
代理程式防篡改功能	✓	✓	✓
App 資產盤點	✓	✓	✓

加選方案

	Singularity Complete	Singularity Control	Singularity Core
Singularity RANGER			
即時全球資產盤點	+	+	+
進階 ML Device Fingerprinting	+	+	+
隔離可疑和惡意設備	+	+	
使用 Storyline Active Response 觀察可疑設備行為並做出反應 (STAR™)	+		
尋找基於設備的威脅	+		
Singularity RANGER PRO			
透過可設定的 p2p 作業自動化降低代理部署落差	+	+	+
Singularity Cloud			
針對 Kubernetes 與 VMs 之 Cloud Workload Security	+	+	+
Cloud 服務供應商之 Metadata 整合	+	+	+
供 Kubernetes 使用之 Automated App Control	+	+	
供 Linux VM 使用的自動化應用程式控制	+		
CIS 工作負載基準 (即將推出)	+		

Global Support & Service Offerings

透過電話、網頁和電子郵件取得技術支援	✓	**包含**
存取產品面的技術資源中心及技術支援網站	✓	**包含**
標準 9x5 技術支援	✓	**包含**
24x7x365 全天候企業技術支援，Sev 1 & 2 全天候服務	+	可選購
指定技術客戶經理 + 企業技術支援	+	可選購
Vigilance Managed Detection & Response(MDR) 訂閱	+	可選購
Vigilance PRO MDR +DFIR 訂閱	+	可選購
SentinelOne Readiness Deployment & Ongoing Health 訂閱	+	可選購

SENTINELONE 全球據點
美國加州山景城（總部） 特拉維夫、波士頓、阿姆斯特丹、東京、美國俄勒岡

全球資料中心
美國、法蘭克福、東京AWS GovCloud
提供您高可用性