SentinelOne

SentinelOne Singularity™

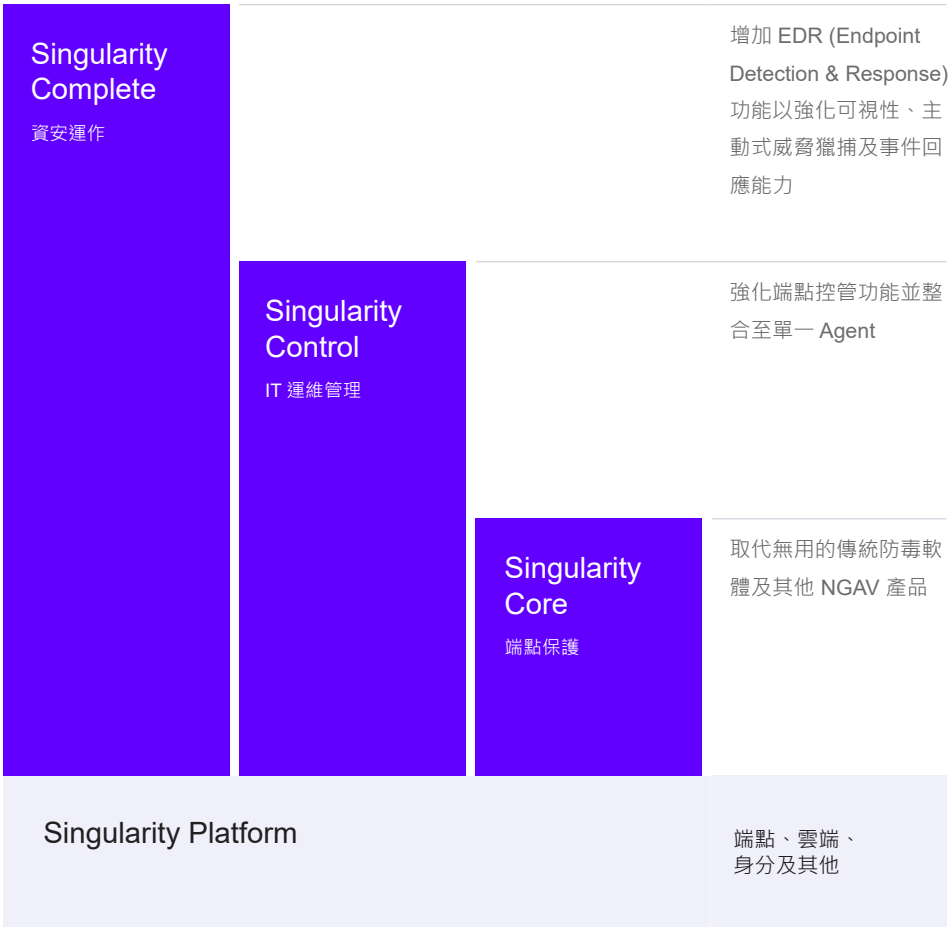
平台套件、模組與服務

SentinelOne Singularity 資訊安全管理平台提供企業 SOC 及 IT 團隊更有效率方式應對日益複雜的資安威脅，以保障企業資訊安全。

SentinelOne Singularity 通過整合並擴展跨多個安全層的檢測和回應能力，包括端點、雲端、身份、網絡和移動設備，為安全團隊提供了集中式的端到端企業可視性、強大的分析和在技術環境的大部分範圍內的自動化回應。

SentinelOne Agent 透過全球各地提供的 SaaS 雲端管理平台統一進行管理，直覺化的操作介面及彈性化的管理方式能應對企業的各式需求。此外，SentinelOne 提供的 Vigilance MDR (Managed Detection and Response) 訂閱式服務更能確保企業的資訊安全團隊得到 24x7 不間斷的支援服務。

本文件將針對 SentinelOne Singularity 不同層級的訂閱項目 - Singularity Core、Control 及 Complete License 進行介紹。每一層級的訂閱項目皆向以涵蓋前一層級的所有功能。



為何選擇 SentinelOne

+ 基於頂尖的 EPP+EDR 技術，SentinelOne 擴展了本地的檢測和回應能力，使其跨越您的攻擊面，實現全球可視性和能力。
+ 95% 客户支援滿意度
+ 96% 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 偵測引擎可有效地阻擋勒索軟體
+ 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程
+ EDR 資料保留期可最高增加至 365 天完整地保存歷史資料
+ 可快速與其他解決方案進行 XDR 整合

Singularity™ 管理平台功能與特色

所有 SentinelOne 企業客戶皆能透過 SaaS 雲端管理平台享有以下功能：

- SaaS 管理平台全球佈署建置、具備高度可用性、可選擇地區包含：US、EU、APAC
- 管理者登入驗證與權限機制彈性調整，可選用登入機制包含：SSO、MFA、RBAC
- 個別管理者權限控制可針對不同企業需求進行調整
- 長達 3 年的威脅事件紀錄
- 高度整合 SentinelOne 威脅情資與 MITRE ATT&CK 威脅指標
- 數據化 Dashboard 視覺化分析資訊安全指標
- 通知選項可針對不同情境調整，並可選擇透過 Email 或 Syslog 發送
- 小型一鍵應用程式的 Singularity Marketplace 生態系統
- 整合式 API 介面提供超過 340 種以上功能

Singularity™ Core

Core License 涵蓋 SentinelOne 所有端點防護產品的最核心功能。對尋求次世代端點防護軟體取代傳統防毒軟體或無效解決方案的客戶，Singularity Core 可提供更有效率且更簡易管理的端點防護軟體 (Endpoint Protection Platform，EPP)。Core License 提供基礎端點偵測與回應 (Endpoint Detection & Response，EDR) 功能更可讓客戶體驗 EPP 與 EDR 整合產品的防護能力。SentinelOne 的威脅情資亦同步整合至端點防護的 AI 偵測功能中。

Singularity™ Control

Control License 專為尋求頂尖端點防護解決方案，並額外針對端點安全性及軟硬體控管等相關需求的企業所設計。Control License 包含所有 Core License 功能且額外提供以下功能：

防火牆控管功能針對端點所在位置設定規則且有效控管進出端點的網路連線行為與方向。

裝置控管能針對 USB 裝置、藍牙裝置及藍牙相關裝置進行存取權限控管。

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已知的弱點清單及詳細資料整合於 MITRE CVE 資料庫中。

Singularity™ Complete

Complete License 專為尋求端點防護、安全性控管及進階 EDR 功能 (SentinelOne 將此技術稱為 ActiveEDR®) 的企業所設計。Complete License 使用到專利技術 Storyline™，自動地將端點系統的處理程序關聯化 (包含重新啟動前後的相關處理程序) 並完整地進行實時紀錄，以提供客戶日後進行調查。Storyline™ 可免除資安團隊在進行事件分析時所耗費的大量時間，並快速地提供事件相關資訊。

- 專利技術 Storyline™ 能快速針對事件進行根本原因分析 (Root Cause Analysis，RCA) 及事件重點關聯。
- 與 ActiveEDR® 整合以強化正常及威脅事件資料的可視性。
- 資料保留選項可滿足各種需求，最長可升級至 3 年
- 應用 MITRE ATT&CK® 技術進行威脅獵捕。
- 管理者可手動將 Storyline™ 資料標記為威脅事件並交由 EPP 功能進行處理。
- Storyline Active Response (STAR™) 可為不同企業量身打造客製化的威脅獵捕處理規則。
- 內建資料收集指令碼以加強可視性和事件調查
- 攻擊事件時間示圖、遠端殼層 (Remote Shell)、擷取端點檔案、第三方沙箱 (Sandbox) 整合.....等其他功能。

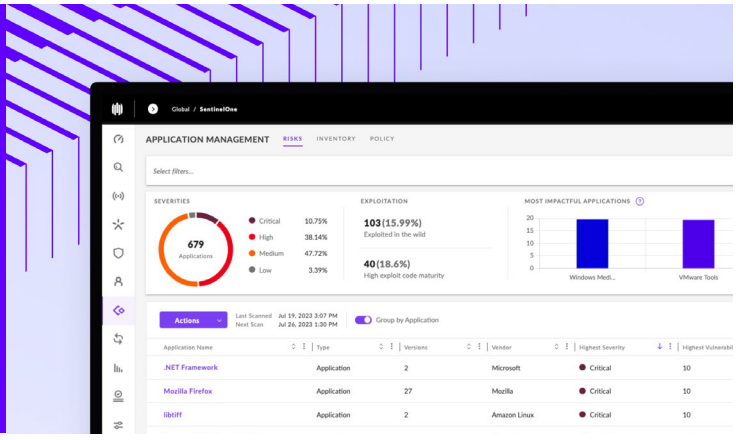
Ready for a Demo?

更多細節

請參考 SentinelOne 官方網站

或致電 +1-855-868-3733

sentinelone.com



Gartner
Peer Insights™

“

令人讚嘆的能力。易於部署和使用 EDR。

網路安全總監

醫療業 1B - 3B USD

Gartner
Peer Insights™

“

SOC 可以仰賴的單一平台。

資安與風險管理

金融業 50M - 250M USD

IT Central Station
Unbiased reviews from the tech community

“

提高效率。我們確實獲得 ROI。

全球資訊安全總監

製造業 10B - 25B USD

SentinelOne 能透過內建的 AI 動態行為偵測引擎有效地阻止勒索軟體 (Ransomware) 及無檔案攻擊 (Fileless Attack)，並具備自動化還原系統功能

Vigilance MDR 訂閱式服務

Vigilance Response　及 Response Pro Managed Detection & Response 是為強化企業安全結構所設計的訂閱式服務。Vigilance MDR 能審查、處理、記錄所有事件並視情況匯報，最大化地提升 SentinelOne Singularity 解決方案的效益及價值。在大多數情況下，Vigilance 分析團隊僅會就重要與緊急事件通知，以確保環境資訊安全。Vigilance MDR 訂閱式服務讓客戶能專注於真正重要的事件上，是幫助降低企業內部 IT / SOC 團隊龐大工作壓力的最有效解決方案。

更多資訊，請參考：
www.sentinelone.com/global-services/services-overview/

SentinelOne GO 訂閱

SentinelOne GO 是為期 90 天的引導式上線和部署諮詢服務，目的是將 Singularity™ Platform 的成功最大化。客戶成功團隊採用結構化方法協助您快速開始運作，並提供最佳實務以長期保持健康度。透過 Vigilance 30 天試用查看成功模式，體驗全代管 24x7 監控與分類。

更多資訊，請參考：
www.sentinelone.com/global-services/readiness/

各層級主要訂閱功能項目

	Singularity Core 雲端原生 NGAV	Singularity Control 安全性 + 套件功能	Singularity Complete 企業安全性
Singularity™ Platform 共同功能			
雲端優先多租戶 SaaS	✓	✓	✓
透過多站點、多群組架構，提供完全可自訂的管理體驗	✓	✓	✓
完全可自訂，以角色為基礎的存取控制和 MFA 整合	✓	✓	✓
獲得專利的 Storyline™ 關聯與脈絡	✓	✓	✓
Skylight 平台資料分析介面			✓
MITRE ATT&CK® 整合	✓	✓	✓
資料在地化	有	有	有
Singularity XDR 功能			
從 SentinelOne 表面代理程式（端點、雲端、身分、行動裝置等）進行原生資料攝入 – 不計量且不會減少 Open XDR 攝入配額。	✓	✓	✓
從任何外部、非原生、非 SentinelOne 來源進行 Open XDR 資料攝入，每天 10 GB。可升級至每天多 TB。		✓	✓
攝入資料保留包括 Open XDR 與原生資料。預設 14 天。可升級至 3 年。			✓
Singularity XDR Marketplace 應用程式		✓	✓
Storyline Active Response™ (STAR) 自訂偵測規則。預設 100。可升級。		僅限 Open XDR 資料	✓
端點層面			
Windows Workstation、macOS 和舊版 Windows（XP、7、2003SP2+、2008）的端點安全性	✓	✓	✓
利用靜態 AI 和行為 AI 提供現代端點保護和 NGAV	✓	✓	✓
自動化或一鍵修復與回溯	✓	✓	✓
威脅分類與調查：1 年回顧	✓	✓	✓
惡意和不安全裝置探索。遠端安裝及其他網路功能需要 Ranger 模組。	✓	✓	✓
行動端點支援：iOS、Android、Chrome OS	⊕	⊕	⊕
EPP 套件控制功能：裝置控制、防火牆控制、遠端殼層		✓	✓
應用程式清單和應用程式 CVE		✓	✓
內建資料收集指令碼			✓
使用 Storyline™ 和 MITRE Engenuity ATT&CK® 對映進行原生 EDR 資料攝入			✓
透過 Skylight 進行原生 EDR 威脅獵捕			✓
原生 EDR 分析			✓

各層級主要訂閱功能項目

	Singularity Core 雲端原生 NGAV	Singularity Control 安全性 + 套件功能	Singularity Complete 企業安全性
雲端層面			
適用於 Linux VM、Kubernetes 叢集以及 Windows 伺服器和 VM 的即時雲端工作負載安全性		✓	✓
自動化或一鍵修復與回溯。遠端殼層。		✓	✓
威脅分類與調查：1 年回顧		✓	✓
雲端服務供應商工作負載中繼資料同步		✓	✓
適用於 Kubernetes 和 Linux VM 的自動化應用程式控制		✓	✓
內建資料收集指令碼			✓
使用 Storyline™ 和 MITRE Engenuity ATT&CK® 對映進行原生 EDR 資料攝入			✓
透過 Skylight 進行原生 EDR 威脅獵捕			✓
原生 EDR 分析			✓
身分層面			
Singularity Ranger AD 模組： 即時 Active Directory 和 Azure AD 攻擊面監控和減少。	⊕	⊕	⊕
Singularity Ranger AD Protect 模組： 即時 Active Directory 和 Azure AD 攻擊面監控和減少，進一步搭配以 AD 網域控制器為基礎的身分威脅偵測與應變。	⊕	⊕	⊕
Singularity Identity 模組： 適用於 Active Directory 和 Azure AD 以及加入 AD 網域之端點的身分威脅偵測與回應。	⊕	⊕	⊕
Singularity Hologram 模組： 以網路為基礎的威脅欺騙，引誘網路內和內部威脅行為者投入並暴露自己。	⊕	⊕	⊕
平台模組選項			
Singularity Ranger® 攻擊面管理模組： 資產探索、指紋辨識和清單。自動化代理程式部署。可疑裝置隔離。轉向 Skylight 威脅獵捕。		⊕	⊕
RemoteOps 模組： 協調鑑識、遠端調查、大規模迅速應變。			⊕
Cloud Funnel 資料湖串流模組： 為了任何目的將遙測資料複製到任何雲端。			⊕
Binary Vault 模組： 自動上傳惡意和良性檔案以進行額外的鑑識分析。			⊕

全球技術性支援與服務項目

	Singularity Core 雲端原生 NGAV	Singularity Control 安全性 + 套件功能	Singularity Complete 企業安全性
標準支援 5/9	✓	✓	✓
企業支援 24/7/365	⊕	⊕	⊕
企業支援 + 技術客戶經理	⊕	⊕	⊕
SentinelOne 引導式上線（「GO」）部署服務	⊕	⊕	⊕
Vigilance Respond 代管偵測與回應 (MDR) 訂閱	有限	有限	⊕
Vigilance Respond Pro MDR + 數位鑑識與事件回應 (DFIR) 訂閱	有限	有限	⊕
WatchTower 主動式活動威脅獵捕與情報報告	⊕	⊕	⊕
WatchTower Pro 客製化威脅獵捕與入侵評估	⊕	⊕	⊕
Vigilance IR 保留服務	⊕	⊕	⊕

圖例：✓ 包含　⊕ 附加元件

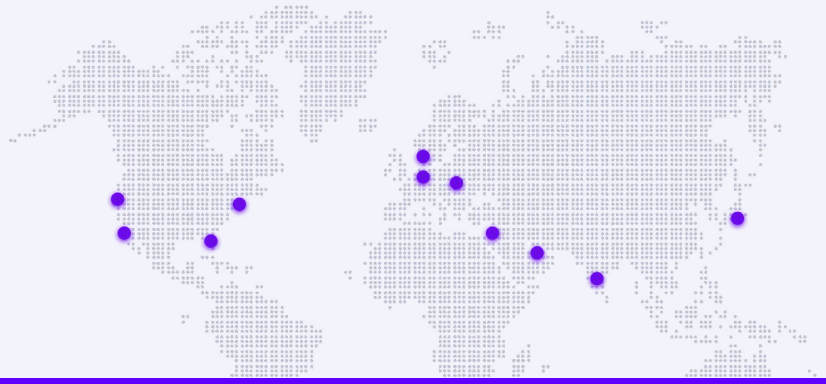
支援地點

美國加州山景城（總部）、阿姆斯特丹、班加羅爾、波士頓、杜拜、尤金、羅德岱堡、布拉格、特拉維夫、東京

全球資料中心

美國、法蘭克福、東京、AWS GovCloud

高可用性



作業系統支援性

SentinelOne 針對 Windows、Mac、Linux 作業系統及其他虛擬化環境提供支援服務。針對各作業系統的軟硬體相關需求，請參見 SentinelOne Support Portal。

Windows Sentinel 代理程式

Windows Workstation 版本自 Windows 7 至 Windows 10

Windows Server 版本自 2008 R2 SP2 至 Server / Core 2019

Mac Sentinel 代理程式

macOS Big Sur、Catalina、Mojave

Linux Sentinel 代理程式

Ubuntu、Redhat (RHEL)、CentOS、Oracle x Amazon AMI、SUSE Linux Enterprise Server、Fedora、Debian、Virtuozzo、Scientific Linux

Windows 舊版代理程式

XP、Server 2003 & 2008、POS 2009

Container 平台支援性

自主管理 (Self-managed) 及託管式 Kubernates 服務 (EKS、AKS、GKE)、Openshift

虛擬化和 VDI 環境支援性

Citrix XenApp、Citrix XenDesktop、Oracle VirtualBox、VMware vSphere、VMware Workstation、VMware Fusion、VMware Horizon、Microsoft Hyper-V

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

代理商 橙鎂科技 sales@ortech.com.tw

+ 886 2 8751 5663

© SentinelOne 2024