SentinelOne | NetFOS 逸盈科技

逸盈科技客戶
專屬限定方案

人工智慧和自動化的深度整合

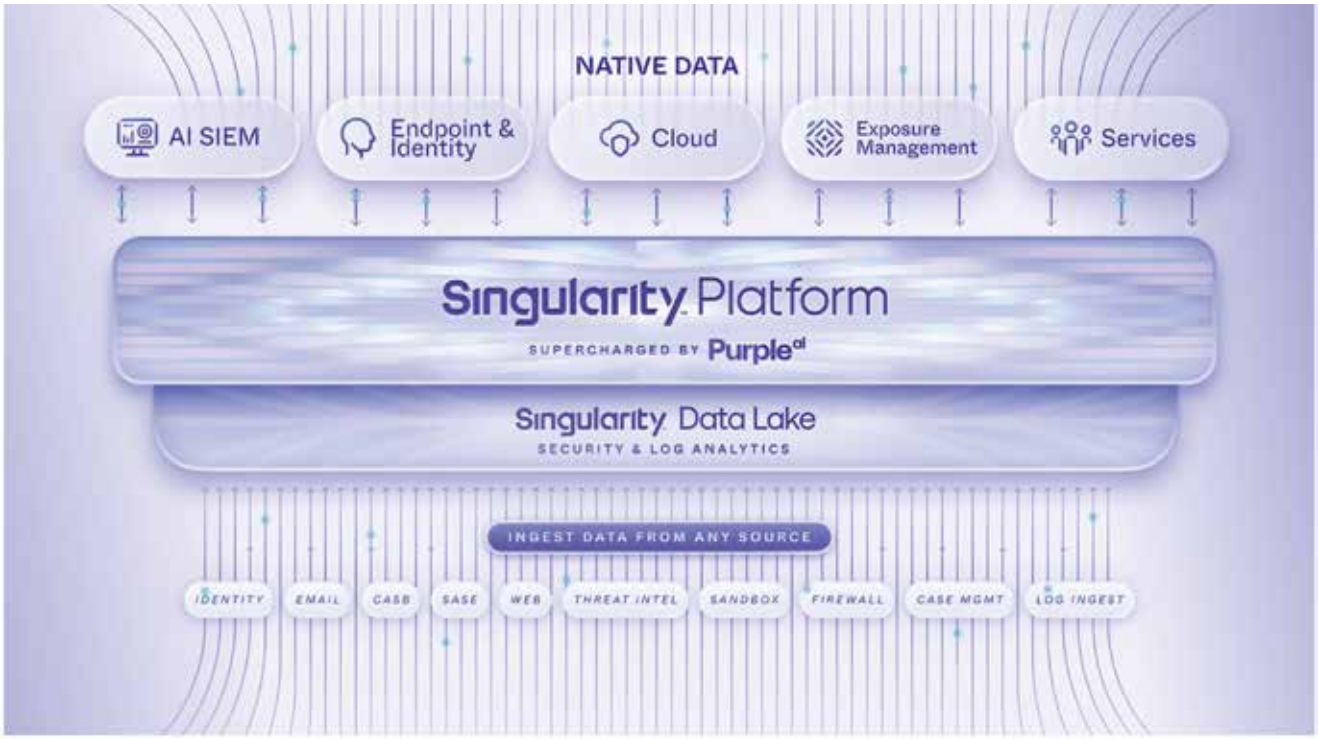
人工智慧驅動的自主防禦正在徹底改變網路安全的面貌，將傳統的被動防禦轉化為主動、快速且高效的自我適應系統。

Singularity™ Platform 透過整合多項創新技術，如 XDR（擴展檢測與回應）、Purple AI、Singularity Hyperautomation、AI SIEM 以及Singularity Data Lake，實現了這一轉變，為現代安全運營中心（SOC）提供了強大的工具，以機器速度檢測、分析並消除威脅。

整合多項創新技術協同運作，推動網路安全的革命

XDR（擴展檢測與回應）Singularity 平台的 XDR 功能超越了傳統的端點保護，將檢測與回應能力擴展到雲端、身份認證和網路連接設備等多元攻擊面。透過整合來自多個來源的遙測數據，XDR 提供全面的可視性，並利用人工智慧快速識別異常行為和潛在威脅。這種整體性的方法讓安全團隊能夠從單一平台監控和管理整個企業環境，減少盲點並提升反應效率。

Purple AI 是 SentinelOne 平台中的生成式人工智慧助理，旨在加速安全運營。它能將自然語言查詢轉化為結構化分析，自動整理事件日誌、提供警報摘要，並引導分析師進行複雜的威脅搜尋和調查。透過自動化警報分類（Auto-Alert Triage）和全球警報分析，Purple AI 能優先處理關鍵警報，減少警報疲勞，讓安全團隊專注於最具風險的威脅，從而大幅提升效率。



Singularity Hyperautomation 引入了無代碼自動化功能，讓安全團隊能夠輕鬆設計和執行針對常見威脅（如勒索軟體、內部威脅）的自動化工作流程。它與平台其他組件（如端點、雲端和 AI SIEM）原生整合，並利用Purple AI 根據同行洞察自動生成應對策略。這種智能自動化不僅加快了威脅修復速度，還減少了手動操作的複雜性，使 SOC 能夠以更少的資源應對更多挑戰。

AI SIEM（安全資訊與事件管理）是一個雲原生、無索引的解決方案，基於 Singularity Data Lake 構建，能夠即時攝取和分析來自企業生態系統的結構化和非結構化數據。它支援開放式架構（如 OCSF），與 SentinelOne 自有產品及第三方工具無縫整合，提供跨環境的即時檢測和快速調查能力。AI SIEM 的自動化功能讓分析師能夠以機器速度應對新興威脅，同時大幅縮短事件回應時間。

Singularity Data Lake（統一資料湖）是平台的數據核心，採用高效的熱存儲技術，支援無限擴展並快速處理來自各種來源的數據。它為 XDR、Purple AI 和 AI SIEM 提供統一的數據基礎，讓人工智慧模型能夠從大量數據中提取可操作的洞察。這種集中式數據管理方式消除了傳統 SIEM 的瓶頸，實現了更快、更準確的威脅檢測與回應。

逸盈科技客戶專屬限定方案

CYBERSEC 2025
現場限定 優惠活動！

凡於現場預購
Singularity™ Complete
50U(含)以上，即享以下好禮

送 Singularity Data Lake
統一資料湖 10G/日(存14日)

送 Purple AI
生成式人工智慧助手

加值服務

歡迎至中芯數據 P305 攤位
進一步了解資安託管解決方案
MDR / XMDR / DFIR / MTHS / IRS 等資安關鍵展示

結論

SentinelOne Singularity 平台透過人工智慧和自動化的深度整合，實現了網路安全的革命性進步。它不僅提升了檢測和回應的速度與準確性，還減輕了安全團隊的負擔，讓他們能夠專注於策略性任務。這種自主防禦模式正在重新定義現代 SOC，使其能夠以機器速度應對日益複雜的威脅，為企業提供前所未有的保護能力。

中芯數據提供 SentinelOne 託管服務，透過我們的專業服務（ MDR、DFIR、MTHS、IRS ），企業不僅能夠精準識別資安風險，還能有效部署強化防護策略，確保關鍵業務的持續安全運行，提升整體資安韌性。

市場認可與技術優勢

Gartner
連續四年被Gartner評為端點防護平台魔力象限領導者

MITRE ENGENUITY
MITRE Engenuity ATT&CK：連續三年取得100%防護與檢測率，並在2022年評比中覆蓋108/109項攻擊技術。

Gartner Peer Insights.
客戶評價中自動化防禦與管理友好度獲高分。