Verint Threat Protection System

一步到位：資安監控中心完整解決方案

現今APT攻擊已經遠超過昔日的惡意程式攻擊。
持續性攻擊針對鎖定目標，利用隱匿技巧滲透網絡，
破壞資安防線，竊取機密資訊。

無孔不入的攻擊方不僅高調滲透業界資安裂縫，近期更將魔爪伸入政府機關，受駭單位包括沙烏地國家石油公司、美國國家安全局(NSA)及白宮。2014年10月皮尤研究中心(Pew Research Center)研究報告指出，60%以上資安專家認為重大資安攻擊會逐漸擴大，其嚴重性將會於2025年危及國安層面。

傳統資安解決方案不堪APT攻擊

您的防護裝置及網路資安工具 (如防毒軟體、防火牆、IPS... 等) 可透過偵測關鍵信號阻擋一般攻擊行動。然而最新的APT攻擊可輕易滲透獨立解決方案的資安漏洞，過時的獨立產品早已不堪攻擊。隨著APT攻擊的形態和方法日新月異，專測個別惡意程式的資安工具呈現越來越多限制。在這危機四伏的時代，企業組織必須透過不同來源的資安訊息，拼湊其關聯性。每日平均1000個資安事件警告已超出各大企業組織的負荷，而SOC團隊根本沒有時間或工具去檢視每一個警告。

獨立解決方案整合成單一整體平台的過程非常繁複且花費驚人。雖然企業組織現有的SIEM系統可以透過現存的系統蒐集軌跡資料，仍無法整合單一攻擊事件做出調查結論，同時無法擴充其他偵測引擎，對於現今的動態威脅也只能望其項背。

主要優勢

- 偵測各方資安系統所遭受的APT攻擊
- 整合多項引擎鑑識調查結果，從單一事件分析提升至預防攻擊
- 利用事件前後蒐集的證據進行多層次動態鑑識調查
- 可行性情資封鎖資安漏洞、鞏固防守結構，預防看不見的敵人
- 公開、彈性、可塑的資安系統結構可不斷增加偵測引擎適應現今動態威脅
- 多項網路和端點引擎的調查結果整合於單一鑑識調查平台，提升資安效率

一刀斃命，戰勝APT

Verint Threat Protection System專門幫助企業組織偵測、鑑識及修復APT攻擊。TPS可監測網路、信件及公司內部流量，監控系統軌跡資料及網路端點，自動偵測以往資安防護無法偵測的攻擊。

資安專家為CSOC資安團隊量身打造的TPS，在各個攻擊環節戰勝APT

- **偵 測** - 靜態檔案分析、動態沙箱分析...等多重檢測方法可偵測零日目標性攻擊，查明確切受害端點。自我學習演算法及行為異常檢測功能有助於察覺未知惡意程式所使用的加密通道與藏匿連線，而網路與端點的全面分析揭露環境內部攻擊的橫向移動，幫助您走在資安防護的尖端。

- **鑑 識** - 透過精密連結、大量資料分析以及優化處理技術，將告警和資訊整合成單一事件，確保您的鑑識分析員能針對重大緊急資安事件進行防護。

- **調 查** - 透過整合網路、端點和軌跡資料工具，單一整合系統可幫助您的SOC團隊即時分析、偵測、對抗威脅攻擊。調查結果根據時間軸、地域、受害清單，以視覺圖表呈現攻擊事件的樣貌。

- **應 變** - TPS會自動產生可行情資來修復被感染的端點與網路，藉由分析結果不斷提升資安設備的防禦強度，避免類似攻擊事件再次發生。

Verint. Powering Actionable Intelligence®.

Verint® Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions for customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in over 180 countries use Verint solutions to improve enterprise performance and make the world a safer place. Learn more at www.verint.com.

info@verint.com
1-800-4VERINT
330 South Service Road
Melville, NY 11747 USA

verint.com　twitter.com/verint　facebook.com/verint　blog.verint.com