

ThreatX by A10 Networks

專為應用程式和 API 防護打造的整合式雲端平台

啟用保護 API 和應用程式的安全性

API 和應用程式的使用量呈爆炸性成長，要應對多向量、長時間攻擊，光是採用特徵碼方法是不夠的。目前複雜的威脅採用 API 濫用、憑證填充、DDoS、漏洞利用、SQL 隱碼和跨網站指令碼等攻擊，持續以資產為攻擊目標。這類攻擊多數由殭屍網路發起，其目的是透過少量和慢速的活動或 IP 輪換等其他技術來逃避偵測。組織可以使用 ThreatX 基於風險的自動防護，以遏止針對 API 和應用程式的威脅。

自動威脅防護

運用基於行為的偵測和自動防護，便能保護 API 和應用程式免受雲端、內部部署和混合環境中的網路威脅。ThreatX 採用流量剖析、集體威脅情報和行為分析的獨特組合，能比特徵碼解決方案更早阻止針對 API 和應用程式的攻擊。此外，我們的專家團隊提供全面託管安全服務，包括主動監控、威脅搜捕、事件回應等，皆有助於減輕資安團隊的工作負載。

基於風險的自動封鎖

ThreatX 平台會自動監控、評估及封鎖攻擊。其會針對威脅樣貌進行學習，然後根據風險等級遏止威脅，使網站保持可用。

防護即服務

我們的安全專家團隊負責主動監控和威脅調查等耗時的任務，能減少誤報並快速應對零時差威脅。

15 分鐘內即可啟用網站，無需數週時間

ThreatX 感測器部署既快速又簡單，還能立即封鎖威脅。只要運用其簡化的儀表板，便能輕鬆專注於針對 API 和應用程式的最重要高風險活動。



軟體即服務



相關的產品與服務



A10 Defend DDoS 防護

深入瞭解

A10Networks.com/threatx

抵禦進階威脅的 API 和應用程式威脅防護

特徵碼方法並不足以抵禦目前複雜的攻擊，唯有靠偵測並追蹤攻擊者，才能防範持續進化的威脅。與其他解決方案不同，ThreatX Protect 是一個完全整合式平台，透過單一解決方案為 API 和應用程式提供抵禦進階威脅與殭屍網路的防護。ThreatX Protect 自動阻止各式各樣的攻擊，確保服務持續可用，永不中斷。



運作方式

- 即時可觀察性:** 平台會根據長時間的行為分析所有 HTTP 流量，查看所有攻擊流量，而不只是一次查看單一事件。
- 探索和編目 API:** ThreatX 會探索每個 API 端點並追蹤接收流量，可標記敏感資料。
- 偵測威脅:** 平台可監視針對 API 和應用程式的攻擊者或殭屍網路，在其嘗試入侵時識別可疑和惡意活動。
- 自動威脅防護:** ThreatX 會根據威脅風險評分自動封鎖及發出警報，不會發生誤報，也無需手動介入。

想要深入瞭解嗎？

立即請求示範，並瞭解如何保護 API 和應用程式抵禦目前的複雜威脅，同時減輕資安團隊的負擔。

深入瞭解
關於 A10 Networks
聯絡我們
apac@a10networks.com

©2025 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 標誌、A10 Control、A10 Defend、A10 Harmony、Harmony、A10 Thunder、Thunder、ACOS、A10 SSL Insight、SSL Insight、SSLi、vThunder、ThreatX 和 ThreatX Protect 是 A10 Networks, Inc. 或其關係企業在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：A10networks.com/a10trademarks。

Part Number: A10-DS-15144-TW-01 Mar 2025

