資料表單

BloxOne® 高階威脅防護

從根本開始加強並最佳化您的資安防護態勢

大規模基礎資安的防護需求

傳統的資安防護模型在當今的數位轉型世代裡已後繼無力。

- 網路邊界已經轉移，您的用戶從任何地方直接訪問基於雲端的應用程式。
- 物聯網的興起導致無法對應傳統端點防護技術的裝置如雨後春筍般暴增。
- 大多數的資安系統都相當複雜，想將這些資安系統擴展到能夠保護這些動態環境所需的等級也不容易。

企業組織們需要的是一個無需進行部署或管理額外基礎架構，即具備可擴展性與自動化機能的簡單資安解決方案以保護整個網路。

INFOBLOX 可提供具備擴展機能的平台，以盡可能地提高威脅防護投資所能為您帶來的效益

Infoblox BloxOne Threat Defense Advanced 是一款全面性的 DNS 偵測與回應（DNSDR）解決方案，可助您偵測其他解決方案可能會遺漏掉的威脅事件，並在這些威脅事件發生之前便透過 DNS 預先搜索威脅情資來阻止攻擊的發生，從而摧毀攻擊者的整體供應鏈。 智能生態系統的整合和自動化機能減少了人工作業的必要，而 Infoblox 特有的 AI 分析資訊能幫助分析師投注心思在最重要的事情上；帶給各位可協助縮短平均修復所需時長（MTTR）、提高現有資安工具投資回報率以及提高整體 SecOps 效率的相關見解。

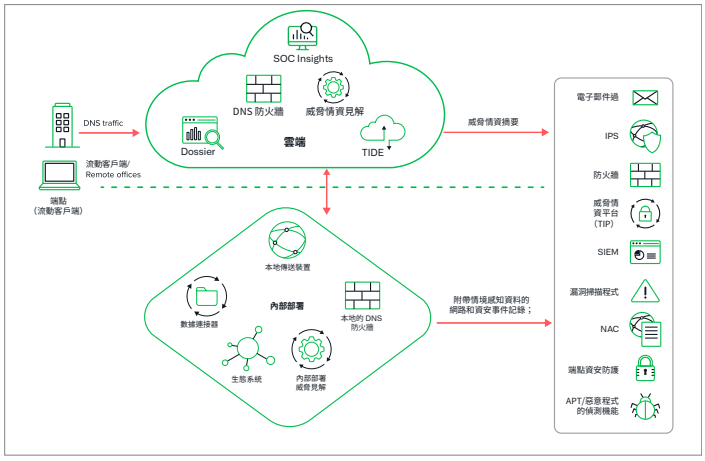

圖 1：Infoblox 混合架構能夠為各位帶來無微不至的防護以及可隨處部署的機能

重點功能

- 偵測並阻止其他解決方案可能會遺漏掉的資安漏洞、網路釣魚、勒索軟體和常見的惡意軟體
- 不論使用的是哪一種平台或是作業系統，都可以自 DNS 層為使用者與裝置的安全把關！ BYOD、物聯網和工業控制系統也包括在內。
- 發現存在高風險的應用程式並管理影子 IT、內部人員、合規性或其他相關的資安風險
- 利用機器學習與 AI 所推演出的分析資料來防範資料外洩的情況發生！舉凡 DNS 面的
- 資料外洩問題 、域名生成演算法（DGA）和 DNSMessenger 等等的情況
- 限制使用者存取不當或不必要的網路內容，並追蹤其網路活動記錄
- 透過監控相似網域來保護您的品牌，並保障您的高價值網路資產
- 將事件調查速度加快 3 倍，並簡化威脅回應和威脅搜索的業務流程
- 提高資訊能見度：透過整合 IPAM 資產元資料來幫助您好好理解事件的來由與其關連性，並藉此取得精準的資安情資以及「和充份的網路情境資料」
- SOC Insights 能夠幫助您快速發起重點威脅的相關調查與事件回應，並透過由 AI 所推演出的見解來縮短平均修復所需時長（MTTR）

最大化安全運營中心效率

縮短事件回應所需時長

- 自動阻止惡意活動，並將威脅資料提供給資安生態系統中的其他成員以進行調查、隔離和修復活動
- 利用網絡和威脅情境情報數據 以及 Infoblox 生態系統集成 (SOAR 的關鍵推動者)，優化您的 SOAR 解決方案 - 減少威脅響應時間和運營支出。
- 超越市面上一般的惡意軟體風險排名儀表板，Infoblox SOC Insights 的 AI 分析資訊能幫助您辨別網路中的重點活動與威脅

透過威脅情報的可攜帶性來統合企業組織內的資安策略

- 同時自內部與外部來源收集並管理威脅情資，然後將這些情資分發到現有資安防護系統中
- 降低威脅資訊的成本，同時提高整個安全系統中威脅情報的效力。

更快的威脅調查和獵殺

- 超越一般的惡意軟體風險排名儀表板，AI 資安見解能夠幫助您針對最麻煩的資安威脅進行快速調查及對應，縮短平均修復所需時長（MTTR）
- 幫助您的資安威脅分析團隊將**工作效率拉高三倍**：透過自動化的威脅調查機能、威脅的相關見解與由數位防護專業團隊所提供的額外研究資料來幫助資安威脅分析團隊針對威脅快速地做出正確的決策

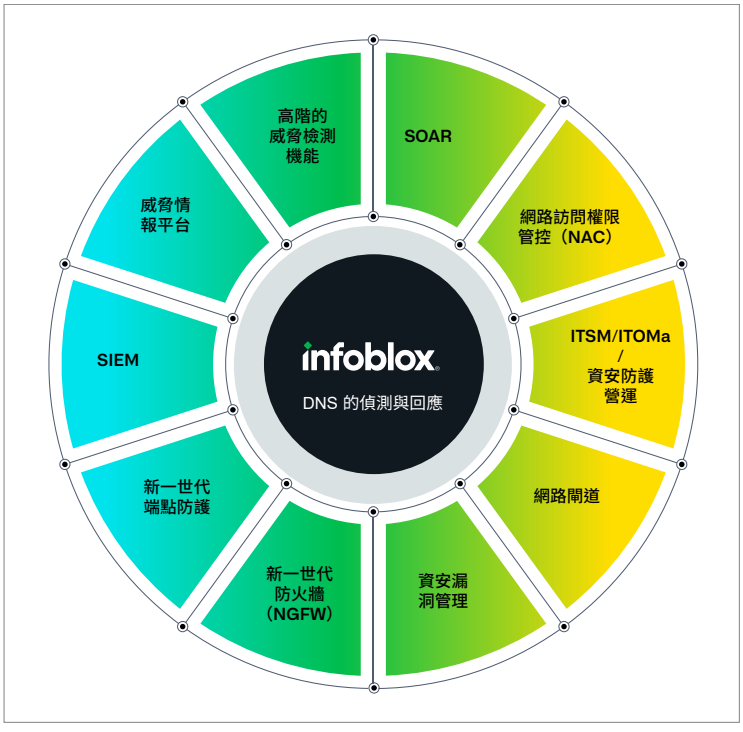

圖 2：BloxOne Threat Defense 與整個網路安全生態系統進行整合

> 「在這個時代裡，有太多的勒索軟體、間諜軟體和廣告軟體會透過網路使用者所點開的連結侵入到各位的網路中。Infoblox 的雲端資安防護解決方案能夠保護使用者們不會因爲重新導向而連上意圖不軌的站點，好防範裝置受到感染，進而保障使用者的安全。」
>
> **美國西雅圖城市大學的資深系統管理員暨網路工程師**

無論您是在哪裡進行部署，混合選項都能夠為您提供防護保障

雲端分析

- 利用雲端更強大的處理能力和基於機器學習的分析技術來檢測更廣泛的威脅，包括數據外洩、域名生成算法（DGA）、快速流動、無文件惡意軟件、字典 DGA 等。
- 偵測雲端中所存在的威脅，並從任何地方強制執行防護措施以保護總部、資料中心、遠端辦公室與漫遊裝置

威脅情資的拓展

- 應用由 Infoblox 研究團隊和第三方服務供應商所提供的全面情資！在本地或雲端實施資安策略，並將對應措施自動分發到資安基礎架構的各個角落
- 無需投入大筆資金為各個站點安裝資安防護措施，即可在雲端中更加廣泛地應用威脅情資

匹配您資安生態系統的強大整合機能

- 透過 Infoblox 和第三方服務提供者的本地資安技術來實現全面性的系統整合，為您帶來全網路的修復機能並助您提高這些技術的投資回報率

遠端生存能力 / 機能彈性

- 如果您不幸碰到網路連線中斷的情況，本地的 Infoblox 系統仍舊可以繼續保護您的系統網路

若想進一步瞭解 BloxOne Threat Defense 是如何保護您的資料和基礎架構的，請造訪：https://www.infoblox.com/products/bloxone-threat-defense

INFOBLOX 資安防護的投資回報率

為集成防護裝置減輕負擔

- 減輕集成系統的壓力
- 將現有的 DNS 伺服器作為第一道防線，並加設防火牆、IPS 和網路代理程式等界限防護裝置
- **通過新一世代防火牆*的網路流量減少 60 倍**

提高既有投資的投資回報率

- 透過雙向共用威脅情資與攻擊發起者的資訊來提高相關/附贈產品的關聯價值
- 如果您現有的方針是將 DNS 資料傳送到 SIEM 進行檢測，或許可以考慮僅將可疑的 DNS 資料傳送至這些平台進行檢測，以降低 SIEM 解決方案的投資成本

自動化機能

- 透過自動化機能來降低人工業務/人為錯誤的成本與代價
- 克服缺乏技術資源的情況讓您的團隊實施（在幾小時內配置，而不是幾個月）和操作需要的技能和成本減少60%。
- 通過簡單容易上手的單一控制台來獲取深度的威脅情資，以幫助威脅情資分析師將工作效率提高 3 倍

*以上皆為實際客戶的數據資料

infoblox.

Infoblox 整合網路和資安防護，為您帶來無與倫比的高效能和安心防護。我們深受由《Fortune》雜誌評所選出的財富 100 強公司企業和新創人士信賴，為各位提供即時的情資能見度與管控機能來掌握是誰或是什麼裝置連上了您的網路，好讓您的企業組織能夠提高營運效率並防範未然。

台灣營運據點
2390 臺北市信義區忠孝東路五段
68 號 29 樓

GCG@infoblox.com
www.infoblox.com

資料版本：20240122v1