Infoblox
CONTROL YOUR NETWORK

DNS 防火牆

資料表

主要功能

- **自適應惡意軟體防護：**偵測並中斷惡意軟體與命令和控制 (C&C) 伺服器的通訊，並降低數據外洩的風險
- **自動化和智能的威脅情報源：**使用自動更新 RPZ 政策的 Infoblox 威脅情報源，提供最新防護
- **與 Infoblox Threat Insight 配合使用時，主動封鎖數據外洩：**將所發現的網域目標新增到黑名單，並封鎖通訊
- **受感染裝置的識別：**利用 Infoblox DHCP 指紋技術識別要修復的受感染裝置，以減少網際狙殺鍊的早期威脅
- **豐富的報告和分析功能來協助修復：**與 Infoblox 報告和分析整合，提供 RPZ 觸發數排行、惡意主機名稱和使用者排行
- **智能的威脅情報：**Infoblox Security Portal 包含威脅查閱工具搜尋引擎，提供有關威脅嚴重性和信賴等級以及威脅內容的可行數據
- **透過與 FireEye 和 Carbon Black 等領先**的安全解決方案整合以及與 Cisco ISE 等 NAC 解決方案交換可行的安全事件資訊來實現自動化的威脅回應

Infoblox DNS 防火牆是基於 DNS 的網路安全領導解決方案，可以有效地遏制和控制惡意軟體通訊，並防止數據外洩，從而保護您的資產和業務。它還提供威脅相關資訊，幫助隔離要進行修復的受感染裝置，並透過自動化的威脅情報源來與不斷變化的威脅格局保持同步。

挑戰

惡意軟體越來越複雜，並且規避了傳統的防禦。根據最近的一項安全研究，超過 91% 的惡意軟體使用 DNS 來獲取命令和控制、外洩數據和重定向流量。傳統的防護方法無法攔截到惡意位置的 DNS 通訊，因此 DNS 安全層是必需的。

Infoblox 解決方案

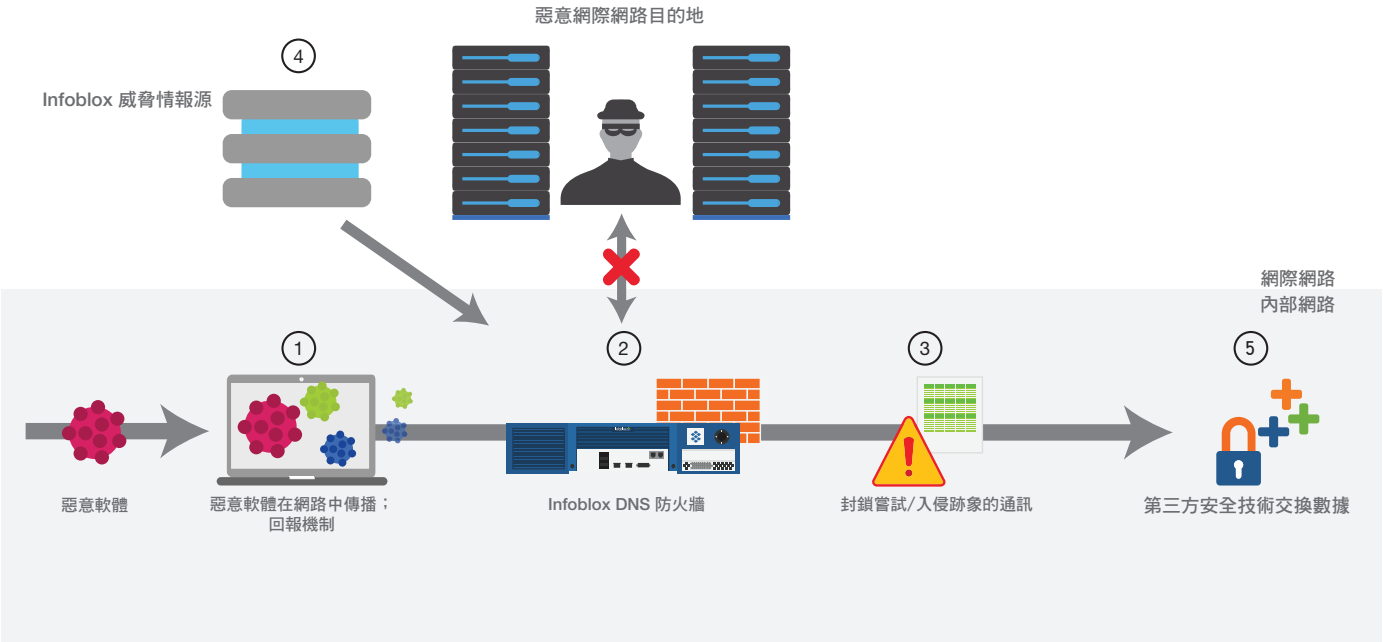
Infoblox DNS 防火牆是基於 DNS 的網路安全領導解決方案，可遏制並控制使用 DNS 與 C&C 和殭屍網路進行通訊的惡意軟體。DNS 防火牆的工作原理是採用 DNS 回應政策區 (RPZ)、智能的威脅情報以及可選的 Infoblox 威脅洞察來防止數據外洩。另外，透過協同使用 Infoblox DHCP 進行裝置指紋識別，使用 Infoblox 身份映射擷取到受感染裝置的使用者名稱，並使用 Infoblox IP 位址管理，DNS 防火牆提供可行的資訊來幫助確定要進行修復的受感染裝置。

此外，Infoblox 還是業界首個且唯一的 DDI 供應商，可將 DNS 防火牆與 FireEye 及 Carbon Black 等領先的安全解決方案無縫整合，並與 Cisco 識別服務引擎 (ISE) 等 NAC 解決方案交換智能的安全事件資訊，以自動化安全回應和隔離受感染端點。

硬體要求	一個或多個配備了已啟用遞迴功能之 DNS 的 Infoblox Trinzic（物理）或 vNIOS（虛擬）設備。 Trinzic 型號： • IB 系列：IB-800、IB-1400、IB-2200、IB-4000 和 IB-4030 • PT 系列：PT-1400/1405、PT-2200/2205 和 PT-4000 • TE 系列（實體和虛擬裝置）：TE-100、TE-810/815/820/825、TE-1410/1415/1420/1425、TE-2210/2215/2220/2225 和 TR-4010/TR-4010-10GE
軟體要求	Infoblox ActiveTrust 標準訂閱授權： • 每個遞迴/轉送 DNS 設備需要 1 個授權（每個設備一個授權，HA 群組 = 2 個授權） • 包括標準維護（Premium、L3+ 等） • 包括 Infoblox 威脅情報源
可選服務	• Infoblox Reporting and Analytics（設備） • Infoblox Threat Insight（軟體授權；需要 Trinzic 設備：IB-2210 或更高版本或 PT-2200 或更高版本） • Infoblox Security Ecosystem Grid 授權：這使 DNS 防火牆可與第三方安全技術（進階惡意軟體防護、SIEM、漏洞管理）相整合。該授權是依 NIOS Grid 提供，成本以 Grid 上的成員總數而異。

DNS 防火牆

資料表



1 帶入辦公室的感染裝置。惡意軟體傳播到網路上的其他裝置。

2 惡意軟體使 DNS 查詢可尋找「home」（殭屍網路/ C&C）。DNS 防火牆查看 DNS 回應，並採取管理員定義的操作（禁止到惡意軟體站點的通訊或將流量重定向到登陸頁面或封閉環境站點）。

3 Pinpoint。Infoblox Reporting and Analytics 列出了 DNS 防火牆操作以及
- 使用者名稱
- 裝置 IP 位址
- 裝置 MAC 位址
- 裝置類型（DHCP 指紋）
- 裝置主機名稱
- 裝置租賃 IP 記錄

4 定期更新威脅情報以獲得最新保護。

5 Infoblox 外來源的其他威脅情報也可以由 DNS 防火牆使用，DNS 防火牆也同樣可與其他安全技術部門分享入侵指標，以增強安全性和緩解事件回應的負擔。

Infoblox
CONTROL YOUR NETWORK

DNS 防火牆

資料表

為何選擇 Infoblox

- 作為企業首選的基礎設施提供者，我們開發了在網路中處於獨特位置的解決方案，以防止惡意軟體。
- Infoblox 將 DNS 通訊協定辨識和高品質的惡意軟體威脅源結合起來，為威脅提供智能的情報和回應，並且無需代理程式，將安全性擴展到網路的所有部分。
- Infoblox 提供第一個也是唯一的 DNS 基礎設施，以使用內建的分析來偵測和封鎖數據外洩。現在，即使在使用最複雜的方法時，Infoblox 也可偵測直接嵌入 DNS 查詢的數據。
- 與 Carbon Black 整合後，Infoblox 客戶可以顯著縮短與 DNS 防火牆警報相關聯的端點回應和修復時間。
- 率先進入市場與 Cisco pxGrid 互聯互通，實現與 Cisco ISE 之間無縫數據交換，提供更高的威脅可見性、更強大的威脅緩解方案以及更高效和有效的事件回應。

主要優點

安全管理員面臨著盡可能快地偵測和應對威脅的壓力。DNS 防火牆透過主動偵測和阻止惡意通訊、提供受感染裝置的資訊，以及隨著威脅的演變發展而調整防護措施，對此工作貢獻力量。

主動

DNS 防火牆是專業的軟體應用程式，利用您已經擁有的 Infoblox DNS 基礎架構，而不是將其捆綁於另一種安全產品上。它解譯每條 DNS 查詢、利用智能的威脅情報來管制裝置到網際網路上已知惡意目的地的通訊，並立即根據 RPZ 政策採取行動。可選用 Threat Insight 會將 DNS 防火牆 RPZ 政策更新為網域數據外洩嘗試相關聯的網域，從而有效防止敏感數據丟失。此外，DNS 防火牆使用領先的安全技術執行即時數據共享，以更快地自動回應和控制惡意軟體。

深入資訊

透過使用自動化的威脅情報源，DNS 防火牆提供了關鍵的威脅深入資訊，可以輕鬆地對感染惡意軟體的裝置排定優先順序並採取行動。透過整合 Infoblox DHCP 指紋技術、IP 位址管理和身份映射，DNS 防火牆可以提供對受感染裝置（包括裝置 IP、MAC、作業系統和類型以及相關使用者）的可見性，以幫助確定要修復的受感染裝置。可選的 Infoblox Reporting and Analytics 提供 RPZ 觸發排行、裝置嘗試通訊的惡意主機名稱、受感染裝置、使用者等的視圖，以幫助您的 IT 安全團隊排定優先順序並快速採取行動。

易調整

利用定期使用新發現的惡意網際網路目的地上的數據進行更新、基於雲端的智能網路情報源，DNS 防火牆可使您的網路保護保持更新。

關於 Infoblox

Infoblox 向全球的企業、政府機構和服務供應商提供智能的威脅情報。作為 DNS、DHCP 和 IP 位址管理 (DDI) 方面的行業領導者，Infoblox 從核心提供控制和安全性，促使數以千計的組織提高效率和可見性、降低風險並改善客戶體驗。

公司總部：+1.408.986.4000　1.866.463.6256（免費，美國和加拿大）info@Infoblox.com www.Infoblox.com