資料表單

Infoblox Threat Defense™ Advanced

防護型 DNS，透過預測式威脅情報，在衝擊發生前保護所有資產、隨處可用

DNS 是所有網路攻擊的第一道防線

DNS 是所有網路攻擊的第一個偵測與預防點。無論攻擊起始於釣魚郵件、簡訊詐騙 (smishing) 或漏洞利用，幾乎所有攻擊都會觸發惡意網域的 DNS 查詢。因此，DNS 提供集中化的可見性與控制能力，保障企業全體：使用者、裝置、IoT/OT 與工作負載，無論是地端、雲端或邊緣。

作為任何溝通的第一步，在 DNS 層偵測並阻擋威脅活動有助於在惡意流量到達下游工具並觸發警示之前阻止惡意流量。透過將 DNS 資料與裝置和資產前後關聯，NetOps 和 SecOps 團隊可以更深入瞭解其環境中正在發生的事情，從而提高營運效率和安全性狀態。

傳統「偵測與回應」方案已不足夠

威脅行為者日益使用 AI 發動更大量、複雜與隱匿的攻擊。他們製造出獨特的單一用途惡意軟體，使得傳統的「偵測與回應」工具—那些等待「零號受害者」感染的工具—無法發揮效用。每次攻擊都會變成「零號受害者」情境，在這種情境下，不存在任何簽章或已知行為。「偵測和回應」工具往往太晚介入攻擊鏈，無法阻止破壞因此需要預防性 (preemptive) 方法，在威脅進入環境或橫向移動前就加以阻止。這不僅可以更早阻止攻擊，而且還降低傳統「偵測和回應」工具的負載。

DNS 作為上游控制點，讓資安團隊能更早偵測並阻擋攻擊，避免其觸及使用者、工作負載或端點

DNS 的預防性安全

Infoblox Threat Defense™ Advanced 提供獨特的 **預先威脅偵測** 方法。這種方法不依賴「零病患」。它使用 **預測性威脅情報 的組合** ，在威脅行為者的基礎架構被武器化之前就加以阻擋，並對客戶網路中的 DNS 查詢進行演算法/基於 ML 的分析，在造成影響之前就提供保護。透過快速識別安全事件所涉及的資產、生態系統整合及直覺的工作區，它能讓您更快速地偵測、更快速地回應，並從您現有的安全投資中獲得更高的投資報酬率 (ROI)。

事實與數據

- 監控 **20.4 萬個** 即時威脅行為者叢集，並持續增加
- 將誤報率降至**0.0002%**
- 在第一次查詢之前已封鎖 **82%** 的威脅
- 平均會在攻擊事件發生前**68.4**天展開防護
- 封鎖**5** 倍於僅檢測已知惡意行為工具的高風險/中風險網域
- 每月平均能省下 **500 小時的 SOC 分析師**工作時間*
- 每年可省下 **$400K**的生產力支出*
- 將數以萬計的警報減少到可以掌握的量*

《The SANS 2025 SOC Survey》的調查報告顯示：在所有會妨礙到 SOC 全效利用的十大障礙中，有八個涉及警報、工具整合和技能短缺的問題

*以上皆為真實客戶的數據資料

在威脅造成影響之前加以阻止

Infoblox Threat Defense 運用預測式 DNS 威脅情報，並透過演算法／機器學習分析即時的 DNS 流量，在威脅影響網路之前就能加以阻擋，往往能偵測到其他工具無法發現的威脅。通過在 DNS 層阻止威脅，Infoblox 還有助於減少下游安全工具的警報量和工作量，客戶報告顯示，下一代防火牆 (NGFW) 和端點檢測與回應 (EDR) 系統的警報減少了 50%

> *「安全 DNS 可降低 92% 的惡意軟體攻擊在特定網路中成功部署的能力」*
>
> **Anne Neuberger，**
> **網路安全部主任**
> **理事會，**
> **國家安全局 (NSA)**

重點功能	說明	Infoblox Threat Defense	NGFW	SASE	EDR
企業範圍的安全解析器和 DNS 查詢記錄	使用 DNS 查詢數據來查找並確定網域。	●	◑	◑	◑
完整的 DNS 行為監控	監控所有的 DNS 記錄類型以檢測惡意活動	●	●	◔	○
仿冒/假冒網域的偵測與取締	緩解相似/冒名頂替攻擊面	●	○	◑	○
零日 DNS 保護	識別可能對您的組織構成威脅的新或新興網域	●	◑	◑	○
基於行為的 DNS 隧道檢測	檢測用於資料外洩／滲透、C2 通訊等的 DNS 隧道。	●	◑	◑	○
主動式可疑／高風險網域保護	預先識別並封鎖可能會在未來惡意活動中使用的可疑網域	●	◑	◑	◑
自動化、原生情境擴充	無需使用者端或是陷坑，即可關聯網路情境（使用者、裝置、來源 IP、位置、MAC 位址、VLAN）	●	◑	◑	◑
主動威脅分佈系統（Proactive Threat Distribution Systems，亦即 TDS）的偵測與阻斷	識別威脅行為者的 TDS 基礎結構，而不僅僅是個別網域，以對應威脅行為者透過在多個網域中進行輪換以逃避偵測	●	◔	○	○

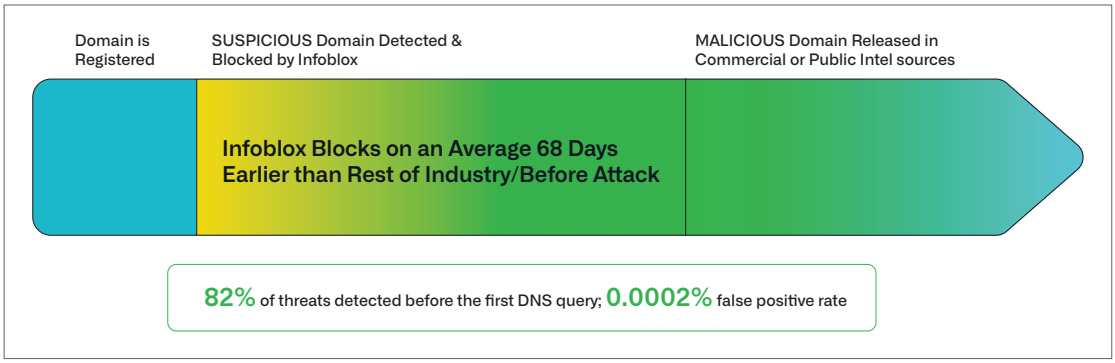
圖 1。其他工具無法完全解決的 Threat Defense 獨特功能

威脅防護的主要功能

- **「防患於未然」監控。**使 CISO 和安全團隊能夠執行其預防性安全策略，並自信地向董事會報告在威脅造成影響之前中和威脅的清晰、可量化的指標——獲得關鍵的時間優勢並減輕安全作業中心 (SOC) 的負擔。
- **資產探索和庫存整合。**快速識別涉及安全事件的資產，以便更快速的事件評估和響應。
- **安全工作區。**簡化直觀的 UI，可讓安全團隊了解其環境中正在發生的事情，並建議降低安全風險的方法。
- **偵測模式。**輕鬆部署和概念證明，而無需更改現有的 IT 或網路基礎架構。

利用預測性智慧提升預防安全性

Infoblox 乃是原版 DNS Threat Intelligence 的領先打造者。該公司採取的是前瞻性而非僅僅防禦性的做法，運用其洞察力在威脅攻擊基礎設施尚在建立時就進行追蹤，並從源頭破壞網路犯罪，往往能在攻擊發動之前就加以阻止。



圖二：Infoblox threat intelligence 可以搶先其他的資安業者防禦威脅

Infoblox 如何打造原版的 DNS Threat Intelligence：

DNS 專家：Infoblox 清楚了解該從何開始著手，挖掘隱藏在 DNS 中的威脅行為者。從高風險或可疑的網域開始，團隊將各個端點串連起來，以識別攻擊者的基礎結構，發現基礎設施並在威脅浮現前提前識別。

威脅專業知識：Infoblox 熟悉惡意行為者的運作方式以及惡意軟體、勒索軟體、網路釣魚和基於 DNS 的漏洞等威脅的表現形式。這些專業知識為預測系統提供支持，可偵測類似網域、DNS 命令與控制 (C2) 活動、註冊網域生成演算法 (RDGAs) 以及其他可疑行為。

資料科學：對大量 DNS 查詢應用機器學習與先進資料科學，實現近乎即時的保護，涵蓋資料外洩、DGA 與各類迴避型威脅

運用 SOC INSIGHTS 更聰明地工作

從警報疲勞和分析師倦怠到漫長的調查和回應工作，Infoblox Threat Defense 透過附加的 SOC Insights 套件為 SOC 提供了顯著的緩解。

- 利用由 AI 人工智慧驅動的分析機能來將數十萬個警報精簡為少量的「資訊見解」，好協助分析人員瞭解最重要的事項。
- 自動化日誌、威脅情報及其他資料的收集與關聯，以便分析師能夠迅速啟動調查與回應。
- 透過資產探索和庫存整合加速事件回應，協助分析師更迅速辨識受影響的裝置。

圖三：Infoblox Threat Intel 分享了驚人的研究數據資料：仿冒網域的資安風險有逐步升高的趨勢

大規模匯出高價值 DNS 日誌

Infoblox 使您能夠輕鬆地將高保真 DNS 查詢和事件數據發送到您的 SIEM、SOAR 或數據湖，以實現集中可見性和更快的威脅關聯。

- 篩選並僅轉送高價值 DNS 事件，降低 SIEM 日誌擷取成本與警報雜訊
- 使用 Infoblox Cloud Data Connector 即時串流增強型 DNS 日誌。
- 為整個生態系中的每個工具提供所需背景，提升偵測與回應能力。
- 與其他工具透過認證的雙向整合無縫共享資料，改善端到端的偵測、分類與回應。

使用 DOSSIER 加速調查

Dossier 為分析人員提供強大的統一研究工具，用於驗證威脅、按照攻擊指標（IOC）展開調查，加速事件處理，無需切換多平台。

- 將內部、Infoblox 和第三方威脅情報整合到一個直觀的介面中。
- 透過內建的增強與關聯分析，迅速調查 IOC 並發現相關威脅
- 避免手動資料收集與情境切換，將調查時間縮短高達 67%。

保護您的品牌免受目標式仿冒攻擊

Infoblox 提供兩項整合功能—仿冒網域監控和網域緩解服務—協助企業防止針對品牌、客戶與員工的仿冒型網路攻擊。兩者結合，可讓您瞭解新出現的威脅，並在惡意網域影響您的業務之前，採取快速、有效的行動對付惡意網域。

假冒網域監控

DNS 是所有網路攻擊的第一道偵測與防禦點

- 偵測註冊來冒充您的公司、供應鏈或面向客戶資產的網域。
- 識別用於針對您的員工或客戶的網路釣魚和詐騙活動的網域。
- 監控高優先級網域的風險狀態變化，並接收即時警報。

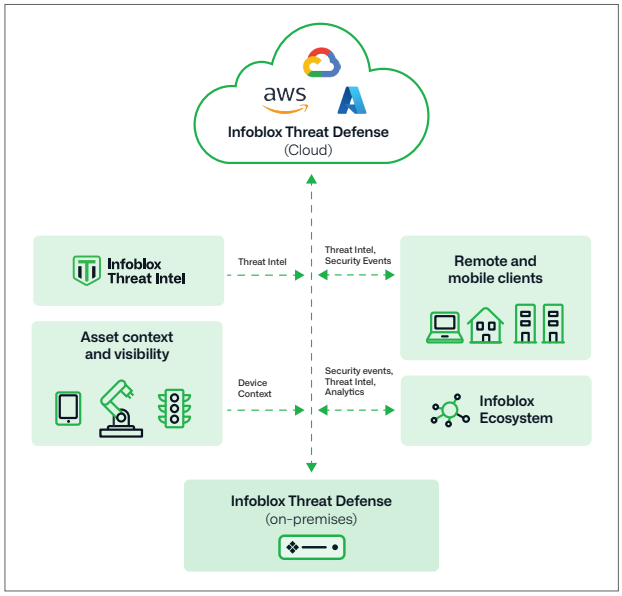


圖 4.Infoblox 混合式架構能夠在任何的地方提供保護和部署機能，好應對當今由 AI 人工智慧所驅動的資安威脅處境。

網域緩解服務

快速驗證並移除在網路上活躍的惡意網域。

- 透過人為主導的事件驗證和摘要報告，確認並記錄惡意活動。
- 與全球 ISP、主機供應商和監管機構協調，以迅速取締，通常在 24 小時內。
- 在移除後的 30 天內監控已緩解的威脅，以偵測並移除重新啟用的嘗試，無需額外費用。
- 解決一系列威脅類型，包括網路釣魚、惡意軟體託管、C2 基礎設施和被盜資料。

若想進一步瞭解 Infoblox 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/threat-defense/。

企業總部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

版本：20250121v1