



保護端點 組織受惠的最佳安全防護 iSafer DNS Booster

數位導向應用與服務近年快速發展，組織或企業不僅是要提升內部 IT、OT 等網路基礎架構的運作效能，也須配合外部用戶需要而提供安全穩定的資訊存取服務，並且還得滿足跨終端載具與系統平台的多元應用，在創造數位經濟效益的同時也帶來更多的資安威脅來源。資安防護好比防盜，需建置多層異質門鎖以降低被入侵受損機會；在眾多資安防護手段中如何就投資成本和防禦效率作出選擇便是門學問。

DNS(網域系統)是組織或企業運行數位服務的最基礎架構元件，它涉及了所有線上的資訊存取服務，包含網站、客服、供應鏈連線、資料備份、語音視訊、文件申辦、安全監控等所有你熟悉的工作要求均須依賴網域系統來指路而開啟各項服務，可謂蛋黃中的核心但卻是所有組織長久來最不被重視的防護項目。駭客組織明白侵入或破壞網域系統就能廣泛性地對組織造成極嚴重損害，勒索即服務(RaaS)的惡意模式便成為暗網世界的新興商業機會，而且是無特定攻擊標的，無論您的組織是哪種產業或經濟規模，都會是名列其中。

您是否正經歷以下未知的管理障礙？

- 01** 知道端點裝置每日連線訪問去哪？
有無記錄可供溯查？
EDR/MDR/SIEM平台僅於資安事件發生後才會告警，對於慣用資安設備(防火牆、網頁過濾、IPS)無法判斷出卻是潛在威脅的連線是不會做出回應並保留溯查記錄。
- 02** 會收到資安事件通報但無法準確找出異常用戶嗎？
通報資訊單只有告知外部DNS非法查詢行爲，組織單位要找出真實內部用戶困難度極大。
- 03** 政府GCB一致性安全黑名單整合程序？
對於國家資通安全研究院(NICS)及金融資安中心(F-ISAC)所供給的IP & URL黑名單需耗時手動鍵入資安設備，且不易探知每次更新差異。
- 04** 恐懼於DDoS攻擊的隨時到來卻不知該如何預防？
添購流量清洗、WAF等服務或設備所費不貲，對於加密流量攻擊亦無法攔阻。

我們著重”預防安全”觀念

URMAZI開發的iSafer DNS Booster系統便是瞄準網域系統安全防禦應用的產品，也是零信任(Zero Trust)框架中訴求終端安全其中一環；iSafer以保護並防堵端點裝置惡意連線為主動手段，進而達到強化企業整體資訊安全性的被動目的，大幅降低外部網路惡意威脅的機會。因為iSafer會在端點裝置向各服務主機發出連線請求時即透過網域代查機制解析連線各項資訊，並依此主動介入安全威脅過濾，同時也將連線內容保留足跡事證。具體優勢包括但不限於：

- ✓ 無須於端點安裝執行或背景程式，不涉及作業系統或版本問題。
- ✓ 無加密性網站過濾阻擋效能障礙。
- ✓ 所有上網連線無論正常或阻斷記錄均被保留，可統合於第三方安全資訊管理平台作為稽核內容。
- ✓ 同步全球上億筆威脅情資內容，有效預防各類威脅連線於請求發起時，而非連線已建立才比對。
- ✓ 限制非產業常態來源網域集中區塊，防止組織暴露於風險來源，縮減風險接觸可能。
- ✓ 透過專屬58類別威脅情資服務能針對特定惡意來源，如殭屍、釣魚、詐騙、勒索、短網址、新活躍域名、加密貨幣等類別威脅阻絕於外。

主要的域名攻擊類型顯著增長

● 2022 ● 2021



域名系統隧道

28% vs 22%



域名釣魚

51% vs 46%



域名惡意軟體

43% vs 38%



零日漏洞

26% vs 23%



DDoS攻擊

30% vs 26%



劫持憑證攻擊

28% vs 25%



雲端錯誤配置濫用

27% vs 23%

iSafer除增強網域安全外，還具備其他較傳統DNS伺服器或次世代防火牆更為先進的管理機制，顯著提升組織內域名服務工作效率與最大可視度，協助IT部門依各任務或安全指標需要去調整管理策略，例如：

- ▶ **DNS Firewall** - 安全協定轉換、ACL管控機制(延遲回應、覆寫、重導向、限量查詢…)、動態查詢阻擋、自訂黑白名單匯入
- ▶ **DNS Server** - 網路多重定址服務、健康狀態偵測、負載均衡
- ▶ **DNS Sinkhole**- 針對特定域名回應錯誤結果屏障危險連結
- ▶ **DNS SafeSearch** - 同步全球主流搜尋引擎平台共同執行最高級內容過濾
- ▶ 即時網域流量資訊看板以及歷史統計報表
- ▶ 支持系統日誌匯出備份
- ▶ 更多進階功能……

總結

網路安全開道產品建置普及的今日，均是著眼在大門的把守和對外偵測機制增加，往往忽略屋內端點本身的行為模式是否會招惹隱性危險，iSafer DNS解析站在最貼近端點的首要數位連線程序，可完全發揮保護端點安全的絕佳優勢且無需為端點安裝外掛或各別設定的額外程序，端點的安全即能為組織整體資訊安全產生極大的益處；”預防安全(Preventive Security)”永遠是為攻擊發生前做最好的準備。

iSafer