White Paper

端點DNS管控

企業資安威脅防護的新管道

當大多數企業依賴次世代防火牆(NGFW)作爲主要的資安防禦基礎設施，受其多元合一的防護功能減輕網路管理單位面對資安技術障礙。但隨著數位資訊的迭代，新的技術和應用也會使得惡意攻擊者利用更智慧的工具創造新的威脅，例如藉由生成AI大量產生變異危害數據，變化之快絕非網管人員或從NGFW閘道設備本體所能及時因應而採取對策，我們需要另一種更快捷有效的方式來強化安全閘道所不足的盲點。

DNS是組織企業既有線上服務所必須使用的基礎協定，其應用範圍如組織內網的印表機，儲存裝置或對外服務的網站主機和客服系統均依賴網域名稱正確解析來建立服務連線，DNS面對連網服務或安全威脅都身在第一線。過往的DNS架構也欠缺自動化與智慧化的資安防禦機制，使得惡意攻擊者也大幅增加針對DNS系統的攻擊，造成企業機密數據外洩影響業務營收以及企業服務可信度的危害，甚至於遭受勒索的極大損失。

iSafer DNS Booster是專屬設計在域名系統安全防禦的解決方案，協助企業將惡意威脅防護能力由閘道移至終端，在內部裝置連網的第一階段即主動過濾與阻擋的安全防護。於此同時，NGFW根本都尚未觸及連線和安全偵測機制，但iSafer卻已經從終端爲您的企業將安全威脅抵禦在外，對各連網終端的DNS活動管控對施以資安防禦，不僅快速有效也可降低企業整體資安防護工作的資源開銷，而這一切將無須介入端點插件的建置或相容性程序。

而DNS層級的防護能力對於遠端或行動終端用戶亦能產生保護作用。因爲用戶處在相對較不安全的公衆網路環境連線至企業網路，遭受攻擊污染的裝置極易將惡意程式散播至企網中，iSafer即可針對以DNS爲基礎的惡意威脅即時淨化與攔阻處理，保護企業網路安全環境 。

功能差異	NGFW	iSafer DNS Booster
防禦時機	連線已被建立或TLS交握發生時。	連線尚未建立前。
過濾對象	URL:檢查HTTP表頭連線已發起。FQDN:須向DNS主機查詢對應的網路位址。	域名查詢時即過濾，防止用戶建立連線。
防護比對數量	上千筆位址或FQDN名稱建立或以TLD爲比對條件，將大幅降低系統效能且手續複雜。	簡單步驟完成TLD過濾設定，萬筆比對數量輕而易舉。
管控機制	僅支持以允許，警告或阻擋的機制。	支持包含允許、阻擋、延遲、複寫位址、複寫名稱、Sinkhole等多元的管控機制。
白名單管理	無相關參考資訊作爲依據。	可爲個體企業產出專屬的DNS活動數據進而打造符合自我需求的白名單政策。
惡意及釣魚攻擊防護	通常以IP爲防護對象，且難就域名識別其安全性。	鎖定惡意或釣魚攻擊域名進行防護，即使關聯上萬IP位址也不影響識別效能。
加密流量檢測	須透過SSL/TSL程序重組封包加解密後才能開始檢測，但已損耗系統大量資源影響防火牆處理效能。	可直接解析DoT,DoH等加密流量並進行安全攔阻，無損系統效能。

iSafer解決方案保護企業的綜合優點

透明化DNS流量提早發掘已知惡意域相關的連接性。

自動化DNS速率限制可以幫助防範DNS放大攻擊並降低DDoS影響。

從DNS活動記錄阻止和過濾訪問有害內容或網路釣魚網站。

支持DNSSEC,DoT,DoH等進階安全協定以確保連線安全。

威脅情報服務以確保已知防護內容的準確性與即時性。

總之，將DNS記錄和配置作爲網路安全策略的一部分，可以幫助您積極保護網路免受各種威脅和漏洞的影響。定期審查和更新DNS安全措施對於應對不斷演化的威脅至關重要。

關於URMAZI Networks Inc.

我們是專精於以網域系統(DNS)爲基礎的資通安全防禦方案的開發團隊，豐富的外商網路安全整合應用經驗。有鑑於網域與線上服務緊密的連鎖關係和威脅影響，開啟我們著手打造符合且眞實解決企業資通安全需要的產品-iSafer。同時，爲能更快速地反應對於未知威脅的前期偵測，我們利用深度學習與人工智慧技術設立專屬的USRA研究小組，提早建立預警情資數據並與全球相關組織進行交換，URMAZI將是您最值得信賴的合作夥伴。

Further Together

