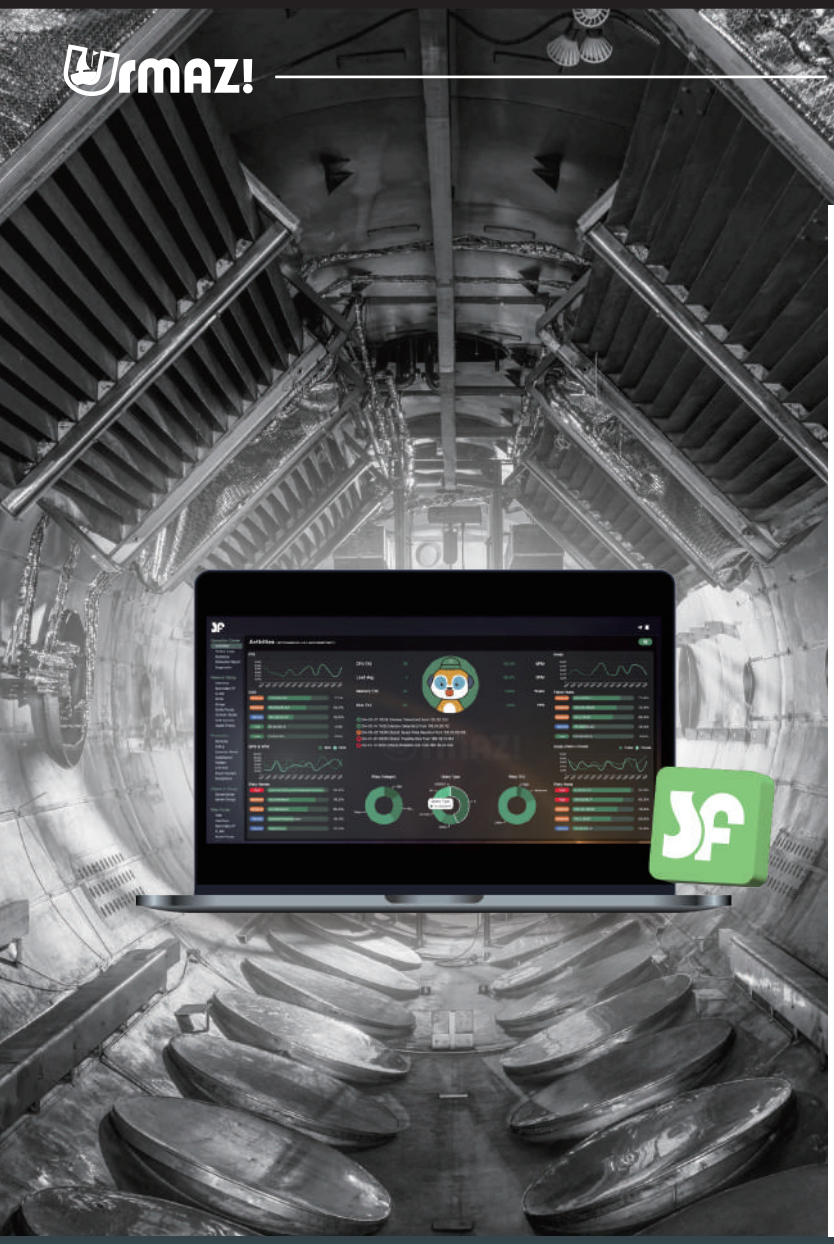


DATASHEET

iSafer DNS Booster

Protective DNS 解決方案

服務性 | 安全性 | 可見性

關於域名系統

域名系統(DNS)是網際網路必用的分層和分散命名系統的基礎協議，用於將人類可讀的域名解析爲數字化的IP位址。它包含一個數據存儲庫是用於存儲域名及其相關IP位址，就像是應用在 Internet的目錄或電話簿一樣，幫助它與企業的網站、聊天機器人、視訊會議、線上購物、客戶服務、網路掛號、網銀交易等依賴網路連線來提供服務的運作密切運作，是組織關鍵資訊基礎設施而需要嚴加保護。

DNS是組織所有對外公開服務的首要接待系統，顯而易見其亦是駭客無差別與零時差攻擊的重要標的，因此，藉由對終端裝置DNS行爲活動掌控後的防護，將是限縮威脅接觸範圍而達到強化整體組織資通安全的有效方式。

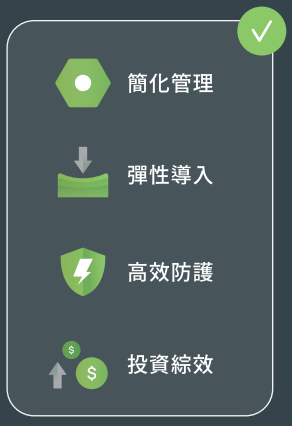
DNS 攻擊威脅風險

根據全球網絡安全威脅報告，基於DNS的攻擊快演進變得高度複雜和龐大，攻擊者大量地採用多元技術且利用不同的DNS元件造成威脅，例如遞回解析器和權威DNS服務器，或是藉由DNS的隱蔽通道進行的數據洩露通常不會被合法的DNS流量檢測到。企業自我檢測和防禦攻擊的難度越來越大，不安全的網域系統的後果將會導致企業處於更高的數據洩露、服務停擺、高額財產損失、法規性失敗和組織名譽受損等不可逆的風險之中。覬覦企業組織因域名系統被破壞後的龐大不法利益，這也是"勒索即服務(Ransomware as a Service)"在駭客集團以商業模式快速拓展的主要動機。

端點安全、組織安全

企業可以在不改變現有網絡環境的情況下，無縫連接並採用iSafer DNS Booster解決方案。iSafer能給您帶來的眞正好處是防止因DNS攻擊造成線上服務的災難，也顯著提升網絡效率和各項業務服務靈活性，爲組織強化安全性、可視性和可控性，讓網路威脅能從一開始的連線階段即被阻擋。

此外，透過URMAZI設立的USRA安全研究學院結合深度學習及人工智慧技術，持續強化未知識別能力並相互交換全球網路威脅情報資料庫服務，保護您的企業免於攻擊的威脅。威脅情資是組織推動自動化與智慧化保護終端用戶避開已知威脅的最有效元素，任何連網載具平台或OS版本或apps 都將與情資緊密結合而得到完善保護。



iSafer 關鍵應用

DNS Firewall

DNS Proxy

DNS Server

Multihoming

Threat Intelligence

URMAZI

iSafer 應用優勢

進階安全協定 Advanced DNS Protocol

在不需要重建或升級既有的域名系統的情況下，支持將加密性DoH、DoT、DNSCrypt的協議內容與傳統DNS協議進行轉換及溝通，確保個人資訊隱私性與傳遞安全性。

惡意來源防護 Malicious Protection

具備58種類別的域名特徵資料庫，快速識別如釣魚、詐騙、殭屍或廣告追蹤等惡意或不當來源威脅，面對加密網站連線也無過濾效能障礙，大幅減輕其他網絡安全設備的解析運作負擔。

全球威脅情資 Global Threat Intelligence

情資必須即時且精準才能有效訂定防禦措施，iSafer從全球蒐集爲數以億計算的龐大網域情資，以及每日平均數十萬筆更新紀錄，不僅是組織安全防禦的標地也成爲掌握組織內部連線分析的重要佐證。

自動學習機制 Auto Learning

動態觀察和分析 DNS 查詢請求和相關回應資訊等內容進行系統自我的學習更新機制。它除了主動對未曾記錄過的域名和回應資訊等組合發出警告外，如果檢測到異常連線就會自動將其添加到白名單中，以便於被控制和同步強化防護能力。

負載平衡與網域多重定址 LoadBalancing & Multihoming

進階的網域名稱服務，讓您可以將公開服務連線平均分配在不同的對外線路。同時，自動判斷並回覆正常運作的線路位址，維持服務不中斷。

網域詢答加速及防護 Boost Queries & Protection

支持查詢記錄和數據封包暫存機制；在遞迴查詢過程中將暫存DNS每一層級的負責名稱服務器資訊，以加快和縮短後續相同查詢的迴應時間和反覆查詢頻率。查詢速率偵測和防護還可以緩解瞬間大量查詢要求，維持公開服務的正常運作。

iSafer 系統平台(選購)

SFMP-1U	1UH,16GB DDR4,512GB SSD,6*Ethernet 1G/RJ45,500W Single PSU

iSafer 產品功能表

產品功能版本	Essential	Advanced	Superior
型號	SF10 / 20E	SF10 / 20A	SF50S
Query per second (QPS)	10k / 20k[a]	10k / 20k[a]	50k
系統服務			
DNS Proxy[b] & Request Route	✓	✓	✓
DNS 服務負載均衡	✓	✓	✓
DNS Server [b]	無支持	✓	✓
網域多重定址[c]	無支持	✓	✓
IP或網域黑白名單與檔案匯入	✓	✓	✓
RRL[d] 支援來源IP、網段、網域	✓	✓	✓
SafeSearch內容過濾	✓	✓	✓
DNS Sinkhole保護機制	無支持	✓	✓
DDoS動態防護			
依查詢數和頻率自定阻擋時間	✓	✓	✓
依RCode回應數和頻率自定阻擋時間	✓	✓	✓
依QType數和頻率自定阻擋時間	✓	✓	✓
DDoS防護政策			
限定查詢閾值	✓	✓	✓
允許、阻斷、延遲、位址或域名轉換	✓	✓	✓
全球威脅情資服務			
Go-start方案 (惡意、釣魚、詐騙類別)	訂閱		
Plus方案 (55類別如勒索、電子貨幣平台、短網址、新註冊等)[e]	訂閱		
最低系統需求：4 vCore , 16GB RAM , 512GB 資料儲存空間, VMWare ESXi v6.5 版本或以上。			

[a] 基礎預設授權爲10k QPS可藉由另購升級授權至20k QPS。[b] 支持服務協定包含 UDP、TCP、DoT、DoH、and DNSCrypt。[c] 預設授權支持2個網域，可另增購升級授權以支持更多網域應用(每單一授權以2個網域爲限)。[d] RRL表示回應率限制(Response Rate Limit)。[e] 訂閱方案包含Go-start類別於授權效期間，若有類別增加將不需支付額外費用即可使用更新。

註：本公司保有上述功能與效能調整的權利而不另行通知。