iSafer DNS Booster

Service optimization and cyber security enforcement

關於 DNS

域名系統(DNS)是 Internet 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。

DNS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。

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，例如遞歸解析器和權威 DNS 服務器。此外，通過基於 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。

iSafer 產品基礎

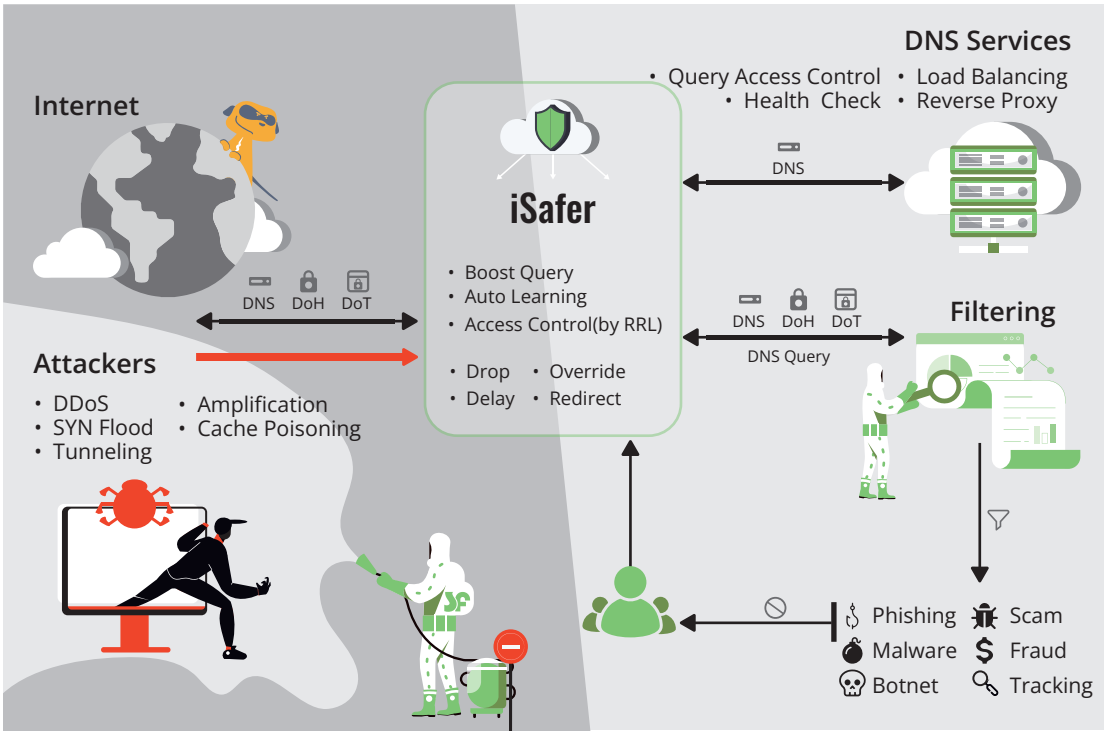
iSafer是一款專門針對DNS服務的優化和安全防護的軟體平台，能有效地提供組織發掘、阻止和減緩網絡威脅的多重能力。全球DNS安全數據顯示，惡意域名的數量每年倍增。因此，安全團隊應該把網域安全作爲首要任務。

iSafer通過對DNS活動進行優化，不僅可以優化公司內外DNS的服務性能與品質，還可以在服務連接的第一階段就進行主動監控和阻止惡意威脅。由於威脅在開始之前就被阻止了，這大大減少了由DNS相關風險(如DDoS、劫持、中毒、隧道)所引起的停機時間，這些網域風險在組織對其安全基礎設施進行維護或建置時通常是被忽略。

Summary

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攻擊造成的災難，顯著提升網絡效率和各項營業服務靈活性。強化企業對於 DNS 基礎服務的可視性和可控性，讓網路威脅能從一開始的連線階段即被阻擋。DNS服務與您的所有線上業務緊密相關。因此，提高DNS安全性和生產力對於您的企業來說是一項緊迫而重要的任務，iSafer所提供的不僅是網域服務的優化者，透過專屬的USRA安全研究學院所提供的全球網路威脅情報資料庫服務，保護您的企業免於暗網攻擊的威脅。

- DDoS Protection
- Load Balance Health Monitor
- Line-Blocking
- DNS Reverse Proxy
- Access Control



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。

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。

網域詢答加速Boost Queries

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。

惡意來源防護Malicious Protection

具備58種類別的惡意對象特徵資料庫，避免遭受像釣魚，詐騙，殭屍或廣告追蹤等惡意或不當行爲所造成的威脅，同時也可大幅減輕其他網絡安全設備的運作負擔。

網域多重定址服務Domain 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。

網域查詢偵測與平衡 Detect & LoadBalancing

不僅是針對分散阻斷式攻擊(DDoS)的進階防護，更支持網域名稱伺服器的負載平衡。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。

Main Functionality

iSafer 產品版本	Essential	Advanced	Superior
產品型號	SF10 / 20E	SF10 /20A	SF50S
過濾效能			
Query / Second(QPS)	10K	10K / 20K	50K
DNS 服務機制			
DNS Proxy[a] & Request Route	V	V	V
DNS Server Load Balance	V	V	V
DNS Server[a]	N/A	V	V
Multihoming[b]	N/A	V	V
DNS 防火牆保護機制			
Access Control by Address and Domain	V	V	V
Custom Blacklist and Whitelist Domains	V	V	V
Custom Blacklist and Whitelist Response Addresses	V	V	V
Domain Name and Address Translation	V	V	V
Mandatory & Custom Response Time Delay	V	V	V
Safe Search Enforcement	V	V	V
DDoS 防護機制			
RRL[c] by Single Source and Subnet	V	V	V
RRL[c] by Query Domain	V	V	V
進階安全威脅防禦機制			
Go-Start Botnet,Phishing and Scam Protection	V	V	V
DNS Sinkhole and Source Tracking	N/A	V	V
55 Plus Categorized Protection[d]	訂閱		
最低系統需求：2 Cores、8 GB RAM、64 GB 資料儲存空間，VMware ESXi v6.5 版本或以上。			

[a] Service supports UDP, TCP, DoT, DoH, and DNSCrypt. [b] Product comes with license of 2 domains. If multihoming is needed to be enabled on more than 2 domains, extra license is required.
[c] RRL stands for Response Rate Limit. [d] No need to pay extra license fee within valid subscription period if number of category increases.

※註：本公司保有上述功能與效能調整的權利而不另行通知

