

# 解決資安威脅的標靶處方

## iSafer DNS Booster

### 21世紀教育產業新挑戰

隨著高速網路的基礎建設完善，以及新世代學子對於電資裝置的高度依賴性，還有近年深刻影響全球的COVID疫情，快速推升網路交流的服務需要如線上教學、視訊會議遠端實驗室、雲端共享、公文簽核、學習評鑑……等等。

當資訊服務便利性被提昇後，資訊安全威脅也就接踵而來，駭客更樂於著墨利用各種資通設計上或行為上的漏洞，尋找對其有利從事不法的機會。當研究計劃或教職學員個資遭受竊取利用，誤導用戶陷入詐騙所造成的信用和財產損失，甚至殭屍控制校務運作，教育管理當局勢必得將資訊安全威脅防護列為工作重點，精進資安治理成熟度以達國家資通安全策略目標。

### 資安威脅有哪些？

資訊安全的威脅非常多元化也包含了內部與外部型態所衍生出的威脅，因此管理當局需藉複合的手段來強化抵禦能力並保護內在資安環境。資安威脅若成事實將對所有連網裝置造成不可逆的影響與災害，大致的種類有：



1. 電腦病毒&惡意軟體



4. 社交工程



2. 網路攻擊



5. 內部人為疏忽



3. 身份盜竊



6. 自然災害

每一種威脅都必須搭配適當且專屬的應對產品或行政措施，才能將資安威脅災害減至最低程度。

### 國家資通安全發展重點

有鑑於所有的Internet服務均須依靠DNS的解析才能成功地運作，就使用者與惡意駭客雙方都需要從DNS服務過程中各自達到目的。現今為數眾多的網安防火牆或網頁過濾產品均是以連線建立後的攻擊特徵與內容而加以比對，進而阻斷的處理模式；有別於上述產品技術觀點，iSafer DNS Booster所採行的是服務發啟的第一關鍵程序 - DNS解析查詢時即介入安全審查，同步阻斷惡意網域連線以保護終端用戶有效降低與威脅的接觸。

數發部資通安全署所發佈的“國家資通安全發展方案“第六期(2021-2024)即明確執行目標-強化外網惡意入侵偵測及區域聯防，並提升網域名稱系統 (Domain Name System, DNS) 抵禦攻擊之抗性，以確保DNS資料之「機密性」與「完整性」，及DNS持續「可用性」。

### 應用都已上雲端，還會有DNS安全強化的必要嗎？

答案是肯定的，主要的技術依據有：

- DNS仍然是網路服務基礎架構中的核心元素，儘管應用服務已經託管在雲端，但仍需靠DNS正確解析而導向到應用服務主機，當民衆因需要而連線到服務系統，DNS的攻擊將導致服務不可用或將連線重新定向到惡意網站。
- 雖然Amazon或Cloudflare等第三方託管服務可能會提供一定程度的DNS安全性，但它們無法保證針對所有類型的攻擊提供全面保護。
- 基於雲端的服務仍然容易受到DNS攻擊，如DNS欺騙、緩存中毒和DNS反射攻擊。因此，實施額外的DNS安全措施以保護您的服務和用戶是必要措施。



## iSafer DNS Booster 應用優勢

正如國家資通安全計劃中所述，iSafer即可滿足其在DNS資料之「機密性」與「完整性」，及DNS持續「可用性」的多樣要求為基本功能表徵。各別的具體做法如下：

### 「機密性」

iSafer支持進階DNS通訊加密協定(DoT / DoH / DNSCrypt)，防止應用服務在網域查詢過程被惡意截取或被竄改，保障詢答傳輸的安全性與機密性。

### 「完整性」

iSafer的處理核心即是針對DNS系統活動執行全時的記錄與監管，不僅可讓網管者掌握詢答過程與內容，更能轉化記錄為相關統計圖表，以利資通安全管理政策的彈性調整和優化。

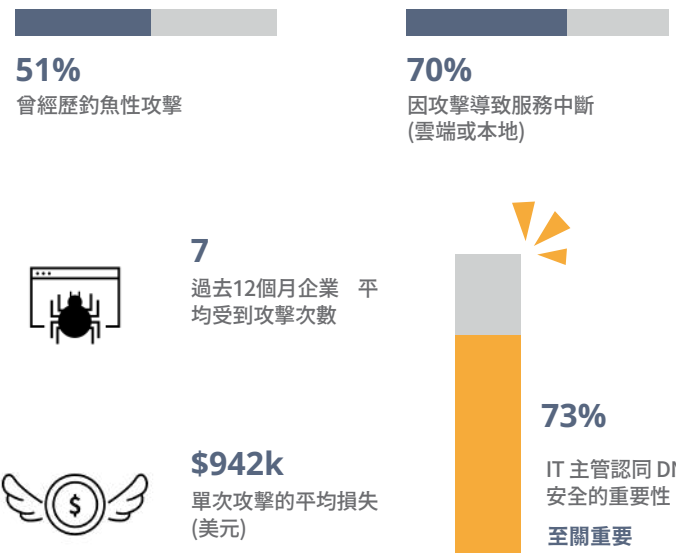
### 「可用性」

外部攻擊者最常利用的即是對DNS系統發動分散式阻斷攻擊(DDoS)，使其系統資源耗盡以致所有依賴Internet的服務中斷，造成極大損失。除此外，在進行大型服務如線上註冊，視訊教學以及報稅…等，會在同一時段湧入大量連線，穩定的服務可用性將是關鍵。

iSafer 提供相對應的機制，如：

- 限定網路來源查詢臨界數量，匹配即自動採取阻斷/延遲/重導/覆蓋等進階保護措施，避免DDoS攻擊產生。
- DNS系統服務負載均衡，以有效降低後端服務主機的負荷，確保提供穩定服務品質。
- 對於陌生查詢或回應變異具備自動快取與學習能力，為可用性建立更快速的反應時間。

## IDC 2022 全球 DNS 威脅報告



iSafer DNS Booster 在教育行業的應用優勢不單是以滿足國家資通安全計劃為限，而是包含其他更多階管理機制及安全防護功能：



#### SafeSearch

網管人員不再需要為連網裝置逐一設定搜尋引擎不當關鍵內容安全規則而疲於奔命，開啟SafeSearch 即強迫連網裝置套用過濾政策。



#### Multihoming

具備健康檢查機制，能大幅降低因單點DNS伺服器故障導致無法連線到各種服務的風險，同時藉由其流量負載均衡的功能也能增強web services 的運作效率，保護服務伺服器的資源不被消耗殆盡。



#### Sinkhole

針對可疑來源施以誘捕，回應預設特定IP以避免讓此可疑來源潛入內網，攔阻後告警用戶異常，同時也能協助網管追查來源與行為模式的安全防護功能。



#### Blacklist

可限制境內外惡意網域名稱或IP位址，作為資安防護的第一線防衛措施。越來越惡意程式及殭屍裝置利用DNS查詢C&C伺服器(Command and Control Server)，Blacklist讓管理者自訂阻擋的網域名稱和查詢回應位址，避免使用者接取惡意或不當的網域名稱或IP位址。



#### USRA

專屬威脅情資研究院具備深度學習及人工智慧技術，以及密切與國際專屬安全情資單位互動交換成果，支持iSafer訂閱用戶獲得最新威脅情報並融合安全管理政策中，動態保障資訊安全防護力。

#### iSafer 多重角色



觀察者



優化者



保護者



AI學習者



分析者

## Conclusion |

iSafer DNS Booster能為教育當局在人力與營運經費資源有限情況之下，提供最直接有效的網路保護性，在不需耗時教育校內所有用戶具備判別連線好壞的專業能力，即能保護用戶避免遭受多樣化的網路威脅攻擊，同時也迎合國家資通發展計畫，建立安全與高效的網路環境及服務。