For Mfg. & Retail

解決資安威脅的標靶處方
iSafer DNS Booster

製造與零售資通安全挑戰

現代化製造業無論是傳產或高科技屬性，均已隨著高速網路的基礎建設完善而大幅增加生產效率及講求自動化與智慧化，帶動零售產業能以更精準與貼近市場的衆多服務創造營收；而全球化營運更需要將服務數位化和網路化而得以快速，準確地推播至各地和終端用戶。無論是生產數據或是用戶資訊，甚至是使用體驗，都是支持經營階層動態調整商業決策的有利工具，使其能擴大商業應用範圍與獲利。

辦公室自動化(OA)，在製造與零售行業中使用OA工具的例子包括：電子郵件、訂購系統、庫存管理、人事資料庫、財務系統、客服系統等等。而營運技術(OT)，在零售業中常指用於POS銷售系統、庫存管理系統等。這些應用服務均與包含大量的企業營運機密，必需加強人員資安危機觀念外，更應強化並建立自動化的資通安全防禦能力將威脅阻絕於外。駭客常藉由入侵系統以控制生產機台，不僅影響生產力或中斷的影響，嚴重的還可能導致人員傷害或致死的後果，這些都將會左右客戶對此企業的商業信譽和合作經驗，也是駭客攻擊勒索要脅的終極目的。

資通安全關注重點

有鑑於所有的Internet服務均須依靠DNS的解析才能成功地運作，就從使用者與惡意駭客雙方其實都需要藉由DNS服務過程中達到各自的目的；使用者需要穩定且安全的服務連線，而惡意駭客則是盡其所能地破壞安全機制以獲取不法利益。

現今爲數衆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所採行的是服務發起的第一關鍵程序 – DNS解析查詢時即介入安全審查，任何威脅將同步觸發阻斷惡意網域連線，在未造成災害前即主動保護終端用戶有效降低與威脅的接觸，保障企業資訊與財產安全。

資安威脅有哪些？

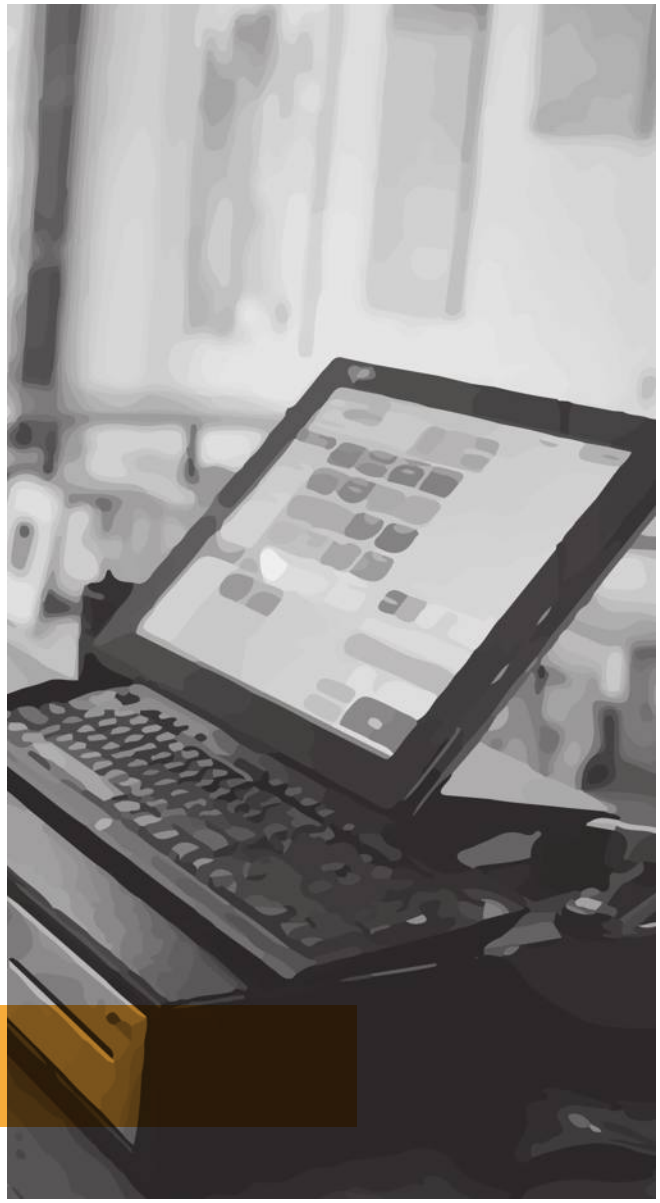
資訊安全的威脅非常多元化也包含了內部與外部型態所衍生出的威脅，因此IT管理當局需藉複合的手段來強化抵禦能力並保護內在資安環境、次世代防火牆、網頁過濾、沙箱……等各式資安產品均有其特定防護專長，難以藉單一性產品而具備全面性資通威脅防禦能力。資安威脅若成事實將對所有連網裝置造成不可逆的影響與災害，威脅大致的種類有：

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。

服務都已上雲端，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　NS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

如國家資通安全發展計劃對於DNS安全防禦耐受力的強化目標，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」的多樣要求爲基本功能表徵。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，更能轉化記錄爲相關統計圖表，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，在進行基礎服務如生產監控，視訊會議以及線上客服……等，都需要穩定的服務品質及可用性均是關鍵。

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，爲可用性建立更快速的反應時間。

iSafer DNS Booster 在製造與零售產業的應用優勢不單是以提昇企業DNS服務效率爲限，而是包含其他更多階管理機制及安全防護功能：

SafeSearch

對於企業內部員工於搜尋引擎進行不當關鍵字詞查找的行爲，網管人員不再需要爲所有連網裝置逐一設定其安全規則。開啟iSafer 中SafeSearch功能，即可統一強制連網終端裝置套用安全過濾政策，快速且有效。

Multihoming

面對全球化競爭，服務的穩定性及不中斷性是企業服務最重要的一環；iSafer具備健康檢查機制，全時偵測服務主機的連線品質狀態，並搭配演算技術適當分配處理進入服務主機流量，不僅大幅降低因單點DNS服務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爲模式的安全防護功能。

Blacklist

可使用自訂格式或利用 RPZ 格式檔案匯入，限制境內外惡意網域名稱或IP位址，作爲資安防護的第一線防衛措施。越來越多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。威脅情資將DNS服務解析責成58類別，580萬筆有效數據且以每日平均3萬筆新增資料速度擴大中，此支持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

良好的網域安全是企業發展各項網路創新服務的基礎，但在全球過去的12個月統計顯示，企業遭受資通威脅主要分佈在惡意網站、間諜軟體、釣魚、DDoS、勒索軟體等外在與DNS服務相關的攻擊模式；這些均可在域名查詢連線過程即可有效被識別而阻斷後續災害發生。iSafer DNS Booster 的設計即是爲您的企業從優化DNS服務並整合威脅情資的安全服務扮演最稱職的幫手，在企業人力與營運經費資源有限情況之下主動站在第一線將惡意威脅阻擋於外，保護內部用戶連線行爲外，更爲企業保障重要資產與營運安全。

