

CHALLENGES

問題及威脅

- 現有資安產品防禦率只有80~90%(可擋已知攻擊及病毒)·對於一到二成的新形態攻擊及勒索軟體無法防禦
- 所有的資安產品都在努力縮短駭客或勒索軟體潛伏時間
- 一旦重要營運主機(SQL、備份或Web Server)檔案被駭客加密或竊取就必須付贖金

SOLUTION

TrustONE 推出「匿蹤防禦」防勒索軟體解決方案

利用TrustONE獨特的「匿蹤保護」技術，採取網路層及驅動層虛擬實體隔離技術，匿蹤保護營運主機的重要檔案，包括：

- SQL資料庫檔案
- 備份主機(Acronis/ Commvault/ Veeam/ Veritas)檔案
- 檔案伺服器檔案
- Exchange郵件伺服器檔案
- AD伺服器檔案
- Hyper-V虛擬機檔案

將重要資料夾設定為「匿蹤保護區」，合法使用者仍然可以正常使用系統與檔案，但駭客及勒索軟體看不見保護區就無從攻擊，避免重要營運主機的檔案被竊取及加密綁架。



「匿蹤保護區」自主保護說明



底層防護

在作業系統的底層進行防護，即便駭客竊取到最高管理者權限也無法移除或修改。



防刪寫

勒索軟體及駭客無法寫入「匿蹤保護區」的檔案，並可自我保護程式及安裝檔不被竄改刪除。

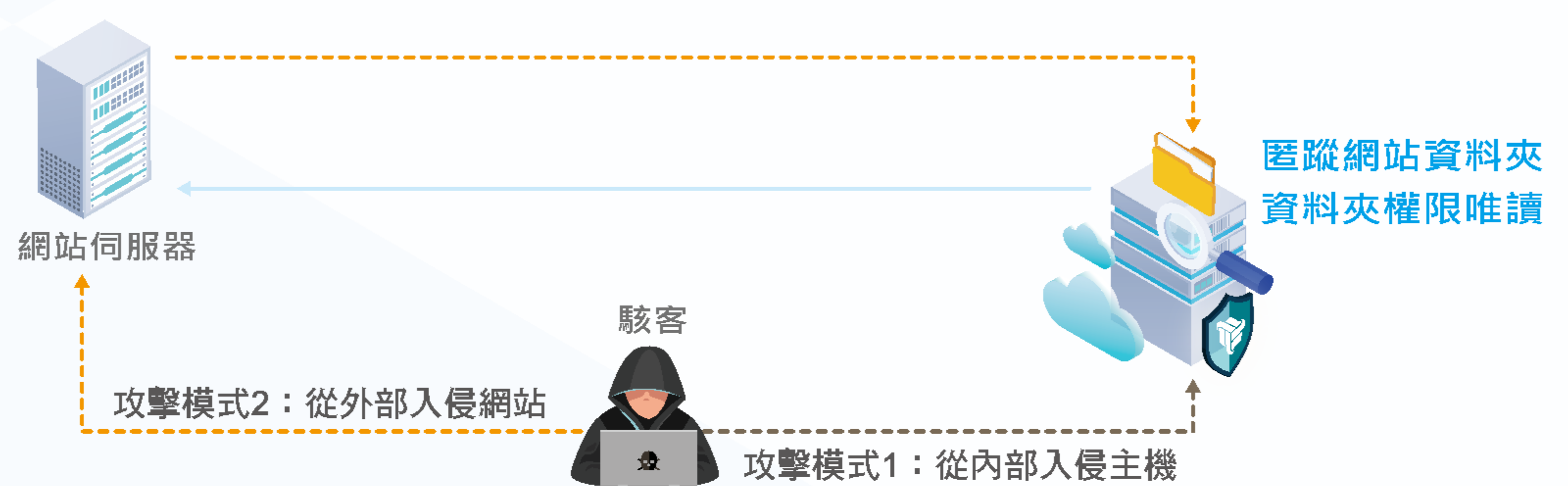


安全程序

可設定「匿蹤保護區」內可執行之應用程式及軟體，因為勒索軟體並不在安全程序清單，就算被有意或無意帶入保護區也無法執行。

防網頁刪除竄改

將網站網頁所在的資料夾設為「匿蹤保護區」，並將保護區內的安全程序設為唯讀，可防止駭客從內部入侵網站伺服器或從外部入侵網頁漏洞，避免刪除竄改網頁、放置惡意程式或植入後門程式等非法行為。



硬體規格建議

TrustONE Server		TrustONE Passport	
安裝環境	建議硬體設備	安裝環境	建議硬體設備
<ul style="list-style-type: none"> Microsoft Windows Server 2012-2019 Standard以上 	<ul style="list-style-type: none"> Intel® Xeon® E-Series 處理器以上 16GB RAM or above 2GB可用硬碟空間 TrustONE Tunnel : 1 Gbps or above乙太網路配接卡 	<ul style="list-style-type: none"> Microsoft Windows 8.1-11 家用進階版以上 	<ul style="list-style-type: none"> 4GB RAM or above 請依作業系統與應用程式官方所列需求 250MB可用硬碟空間卡

業務洽詢

劉先生 (02) 2656-5656 #805 marshall.liu@zerone.com.tw
王小姐 (02) 2656-5656 #213 arisa.wang@zerone.com.tw