

零信任匿蹤聯防

深化核心資料保全

匿蹤區域防禦-保護重要資料預防加密勒索攻擊



1. 現行資安產品對已知攻擊與病毒只能達到八成的防禦效果，對剩下兩成的新型態攻擊及勒索軟體則無法有效預防。
2. 若駭客竊取到系統管理者的帳號密碼，現行資安產品幾乎束手無策。
3. 危機四伏的遠端桌面連線，成為企業深陷資安風險最大夢魘。
4. 駭客經IT入侵攻擊OT系統，伺服器農場(Server Farm)資安岌岌可危。
5. 網頁程式遭惡意異動事件頻傳，WAF及網頁復原產品無法有效保護動態網頁。

針對近年常見的駭客手法（如：使用WebShell惡意指令竄改攻擊網頁），TrustONE能有效的保護**動態網頁**，避免駭客藉由網站的**上傳/下載**功能，或是**服務信箱**等管道進行攻擊。

五大護法 **PROTECTION**

護法 1. 隱藏

- 擔心駭客從動態網頁中的“上傳/下載”功能或“服務信箱”的途徑竄入嗎？TrustONE可直接將關連目錄隱藏保護起來，讓駭客無從下手。

護法 2. 管理者OTP

- 系統管理者帳密被盜了怎麼辦？別擔心，TrustONE用OTP雙因子認證，為主機加上第二道鎖。

護法 3. 唯讀

- 靜態網頁需要百分之百的保護方案嗎？沒問題，如同燒製成光碟片般，TrustONE提供唯讀功能，強化防護重要網站。

護法 4. 復原

- 以不變應萬變，TrustONE隨時偵測檔案完整性，一旦發現被惡意竄改時，立刻將檔案復原。

護法 5. 主動警示

- 百密絕不容一疏，TrustONE二十四小時監控保護Web主機，當察覺威脅發生時主動警示，不放過任何可疑情況。

MANAGEMENT 三大協同管理

管理 1. 異動記錄



提供詳盡檔案異動紀錄（涵蓋正常版更與非法異動狀況），以因應上級機關資安稽核要求。

管理 2. 自動化版更



提供API與指令規則以利整合部署網站更新程序，並符合CI/CD自動化上版流程的需求。

管理 3. 版本控管(選購模組)



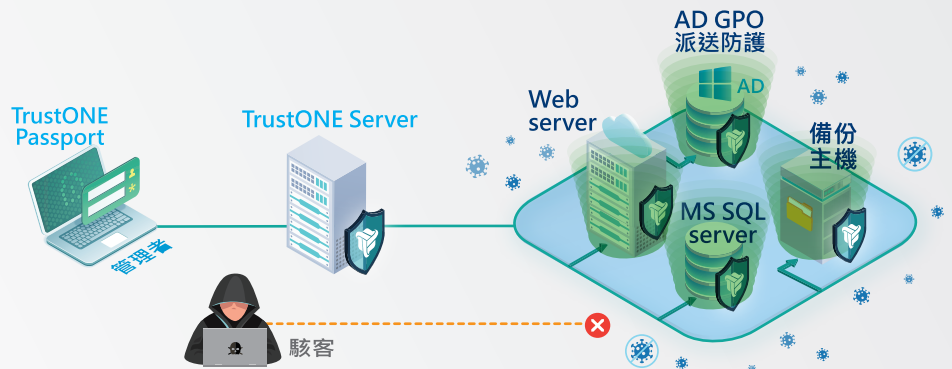
提供網頁上版更新追蹤紀錄功能，方便日後控管網站更新維護之記錄。



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
- 網頁伺服器檔案
- AD GPO群組原則目錄

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。



TrustONE 零信任安全代理

保護遠端桌面/老舊主機/產線機台

零信任安全代理主機

功能 A.

與傳統跳板機最大差異在於採用直覺式連線轉向操作，毋須在跳板機上執行遠端連線工具，可有效節省CPU效能及網路傳輸量。

零信任管理者身份確認

功能 B.

合法管理者必須要以TrustONE Passport通過身分驗證後才能連線使用。驗證方式可使用OTP雙因子認證（Email或手機APP接收一次性驗證碼）方式，可有效阻擋駭客竊取管理者的帳號密碼入侵。

零信任安全應用程式

功能 C.

將合法連線工具事先加入白名單中，TrustONE Server只允許使用白名單中的安全使用程序連線至營運主機，可有效防止駭客使用不明工具入侵破壞。

零信任安全網段

功能 D.

針對使用Server Farm架構或產線環境，可透過TrustONE Server製作隔離保護區，如同跳板機方式使後方形成安全的區段，駭客就算駭進公司網路，也看不到被區隔保護在安全IP及網段中的主機。

零信任主動警示

功能 E.

與TrustONE Server搭配使用，可阻擋未經授權之網路連線，將駭客非法連線的行為事件記錄、威脅情資提供給管理者，追查駭客潛伏位置。



TrustONE Server
零信任安全代理主機

TrustONE
Passport

系統管理者/使用者

► 對應網頁竄改攻擊 / 非法入侵的深化核心資料保全方案

【SQL/備份主機匿蹤區域防禦】

安全程序與雙因子驗證，保護營運主機核心資料，避免駭客進行勒索加密

【零信任安全代理】

建構安全連線通道與強化管理者身分辨識，預防駭客橫向攻擊其他營運主機核心資料，保護遠端桌面

【WAF+弱點掃描】

使用特徵碼比對及行為模式分析技術，針對新型態駭客攻擊會有漏網之魚。

【防網頁竄改】

隱藏 / 唯讀保護重要網頁資料夾，讓駭客找不到下手目標，預防駭客惡意置換網頁檔案及程式

【防AD惡意派送】

隱藏/唯讀GPO群組派送原則檔案，並搭配雙因子驗證，阻絕駭客透過AD管理者帳密派送惡意指令進行勒索加密

TrustONE 硬體規格建議

TrustONE Server 系統需求

安裝環境 (VM亦可)

- Windows :
Server 2012 R2-2022 Standard以上
- Linux :
Ubuntu 20(含)以上
Cent OS 7(含)以上
Red Hat 7.9(含)以上

建議硬體設備

- CPU : 4核心
- RAM : 16GB or above
- Disk : 100GB可用硬碟空間
- TrustONE Tunnel :
1 Gbps or above乙太網路配接卡

代理商

ZERONE
| 零壹科技 |

www.zerone.com.tw