TrustONE

主動防禦

Stealth and Active Defense

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
- 常見駭客攻擊手法是拿到系統管理者帳密權限後再進行攻擊

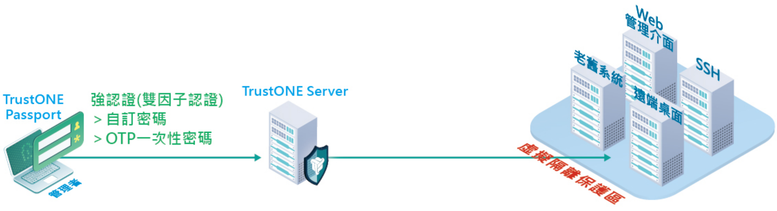
SOLUTION
TrustONE 營運主機守門員計畫

1. 跳板式主機OTP

A. 主機系統管理者透過TrustONE Entry，取得TrustONE OTP雲端服務傳送的APP或E-mail驗證碼(雙因子認證)。

B. 通過身分辨識的合法管理者，可經由TrustONE server進入營運主機管理介面。

C. 就算駭客取得系統管理者的帳號密碼，如果沒有通過TrustONE OTP強認證流程就無法進入營運主機管理介面。



2. 遠端桌面連結營運主機防護

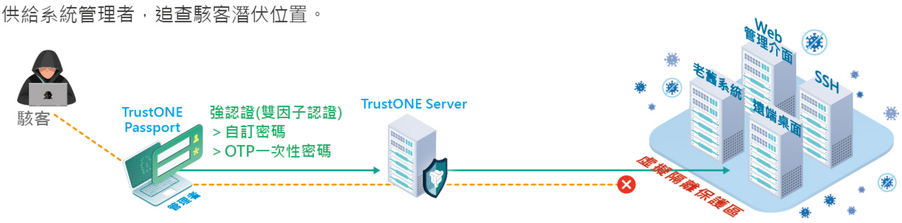
透過遠端桌面工具連結到後端主機存取檔案前，必須先通過TrustONE Server的OTP雙因子認證。未通過驗證者，即使取得管理者帳號密碼也無法成功連線。

3. 跳板機虛擬隔離區

跳板式OTP機制提供跳板機功能，建置虛擬隔離區，將既有環境內的營運主機納入虛擬隔離保護區內，再加上雙因子或多因子OTP身分辨識流程，避免保護區內的營運主機遭受駭客或勒索軟體攻擊。

4. 主動警示威脅情資

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紀錄、威脅情資提供給系統管理者，追查駭客潛伏位置。



硬體規格建議

TrustONE Server	
安裝環境	建議硬體設備
■ Microsoft Windows Server 2012-2019 Standard以上	■ 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

TrustONE Passport	
安裝環境	建議硬體設備
■ Microsoft Windows 8.1-11 家用進階版以上	■ 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

TrustONE 碩壹資訊股份有限公司 | ZERONE 零壹科技