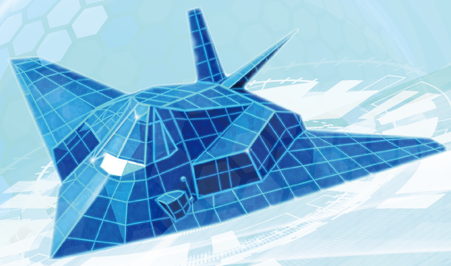
TrustONE

零信任匿蹤防禦

零信任 Zero Trust

匿蹤 Stealth

AI預警 AI Warning



防禦概念：如同匿蹤戰機，敵人看不到就無法攻擊
You Cannot Hack What You Cannot See.

二不：「匿蹤」及「多層次」防禦策略

即使駭客已經入侵，讓駭客 **連不到** 也 **看不到**

零信任 Zero Trust

- 全台首家一次通過資安院三階段認證
- 身分鑑別/設備鑑別/信任推斷
- 同時支援TCP/Web系統，系統提權再認證
- 從PC -> 零信任 -> 主機登入，僅需一次身分認證

匿蹤 Stealth

- 系統底層防護–讓駭客看不到主機檔案
- 動態存取控制–讓駭客連不到重要主機
- 保護核心主機(資料庫/備份/Web Server/Hyper-V/AD GPO)

AI預警 AI Warning

- 同時蒐集與分析Client端身分/設備與Server端主機存取資料
- 整合SIEM/SOC或其他資安系統(例如EDR)
- 提供「人」及「AI agent」異常行為預警，攔阻潛在威脅

TrustONE 碩壹資訊 | ZERONE 零壹科技 | 通過FIDO2國際認證

www.TrustONE.com.tw
service@trustone.com.tw

三階：零信任三階段認證

全台首家一次通過資安院零信任三階段認證 FIDO2 CERTIFIED

身分鑑別	• 支援FIDO無密碼 / MFA多因子驗證 • 可整合Windows Login與遠端桌面
設備鑑別	• 驗證設備健康狀態與合規性 • 確保僅有授權設備能連接內網
信任推斷	• 持續監控使用者連線操作行為 • 根據即時風險評分，與動態調整權限

差異化與優勢

- **同時提供TCP/Web連線機制** — 唯一同時支援Web 與 TCP (RDP/SSH) 系統防護，讓資安零死角。
- **提權再認證** — 執行提權或敏感操作時自動觸發二次認證，確保提權指令皆為本人授權。
- **操作方便簡單** — 從 PC 端點、零信任到核心主機的登入僅需一次驗證，大幅提升操作方便性。

七柱：零信任框架七大支柱

TrustONE支援美國NSA資安指引七大支柱

01. USER
TrustONE身分鑑別
FIDO/APP/Passkey (資安院、金融行動2.0)

02. DEVICE
TrustONE設備鑑別
TPM註冊/設備健康度 (資安院、金融行動2.0)

03. APPLICATION & WORKLOAD
TrustONE應用程式鑑別
版本/簽章/參數/程序 (金融行動2.0)

04. DATA
TrustONE匿蹤防禦
檔案防竊取/防加密/防竄改 (金融行動2.0)

05. NETWORK & ENVIRONMENT
TrustONE網路微分割
阻斷非法惡意連線 (金融行動2.0)

06. AUTOMATION & ORCHESTRATION
TrustONE信任推斷
動態驗證存取權限 (資安院)

07. VISIBILITY & ANALYTICS
TrustONE AI預警
監控智慧預判告警

匿蹤防禦，保護核心資產

- **保護核心主機**
  核心主機重要檔案就地匿蹤保護。
- **系統底層防護**
  合法的應用程序加入安全清單，系統運作如常。
- **動態存取控制**
  駭客看不到核心資料，無法加密、篡改、竊取。

AI 預警 主動式防禦

- **即時聯防**：連動 SIEM / SOC 與 EDR，主動偵測人與 AI agent 的異常行為。
- **AI agent 深度安全治理**：提供 AI agent 操作者的身份鑑別、AI agent 所在端點的設備鑑別、NHI（Non-Human Identity）管理機制，結合人為審查流程（MITL：Man In The Loop），強化安全存取目的 Server 與時間範圍，並同時匿蹤保護 Rule 及 Skill 檔案夾，避免被駭客攻擊。
- **預防性阻斷**：在威脅擴散前精準攔截，讓企業機構無後顧之憂地擁抱 AI 自動化。

零信任匿蹤防禦十大應用

1. 獨家 主機匿蹤(防加密、防竄改及防竊取)
2. 獨家 登入僅需一次驗證(一條龍)
3. 獨家 管理者提權再認證
4. 分權存取控管(RDP/WEB 連線)
5. 強化Windows Login驗證
6. 保護SSL VPN
7. 多因子身分驗證
8. File Server檔案存取軌跡
9. 側錄監控告警
10. 外部連線管控(申覆流程)