Arrosoft SOLUTIONS

Air Gap Ready

OUR SOLUTION

AirGap Solution
離線備份軟體
介紹手冊

Arrosoft SOLUTIONS

AirGap

Arrosoft Solutions-AirGap
謹代表Arrosoft solutions
感謝您有機會協助您利用我們的AirGap方案以及Honey Pot file distribution
和Business Logic Worklows，為用戶端平台部署Arrosoft AirGap解決方案。

在這個變革時代，每個企業現在都是數位化的。企業在網絡安全防禦和威脅檢測方面進行了大量投資，有太多眾所周知的和全球性的網絡攻擊者無法預期。

「AirGap離線備份」是最後一道防線，僅在所有其他恢復手段，已變得無能為力，且無法用於恢復時使用，必須有離線（Isolation）技術架構，來確保在任何情況下都可以還原乾淨的數據。

這個想法很簡單：重要企業數據的安全時間點副本保存在存儲環境中。環境通常與主要生產網絡隔離。保管庫通過受限連接，定期連接到生產環境，以製作企業數據的時間點副本。在恢復過程中，這些解決方案僅允許通過保管庫中的物理狀態訪問受保護的數據，從而保護保管庫免受可能散佈在整個網絡中的任何惡意
代碼的侵害。

- **Method 1: Monitoring the Honeypot File 誘捕系統監視蜜罐文件**

  軟體部署使用蜜罐文件方法自動檢測客戶端計算機上是否存在勒索軟件。 勒索軟件檢查每4小時進行一次。通過發送警報並顯示事件消息，立即通知控制台管理員。

- **Method 2: Detecting File Anomalies On Client Computers 檢測客戶端上的文件異常**

  存在勒索軟件惡意軟件而在客戶端上創建、刪除、修改或重命名了大量文件。 默認情況下會監視這些活動。每5分鐘檢查一次客戶端上的文件活動，並通過警報和事件將任何異常活動報告給管理員。7天中，將對客戶端進行日常活動的監視和分析，而後將建立文件活動的基準，並在檢測到大量異常文件活動時將警報和事件發送給管理員。

- **Method 3: Random Port Opening Times 不定時地開啟增量備份**

  系統備份排程幾乎為固定無法更動的。當駭客得知備份主要工作區的備份時間，便會偽裝成各式病毒侵入備份空間。而不定時的存儲技術為特別開發，能大大降低感染勒索病毒的風險，並加速重複數據刪除後的數據，在備份上有足夠且完美的效率。

- **Method 4: DR-site Control Over Data 備份主控權的對換**

  過去主要活動的Production Site為主要傳輸主控權，AirGap使之對調，讓DR（Disaster Recovery）備援區為主控權，透過前面的所有方法，讓備援區享有選擇資料的權利，避免異常數據的活動。

- **Method 5: Zero Trust Concept 零信任概念**

  由Arrosoft Air Gap系統控制權限 No AD, No Router, No DNS，病毒無權限進入。全球最新企業零信任概念，無權限設計，為珍貴資料創造最乾淨、最純粹的備份空間。

AirGap

美國傲索科技有限公司
Arrosoft Solutions （U.S.A.）
100 Wood Ave South, Suite 119,
Iselin, NJ 08830

Arrosoft Solutions（台灣）
T：(886)-2-8771-0284
M：apac@arrosoft.com
新北市永和區永和路一段158號8樓之3

硬體建議需求：
Air Gap Proxy Server/ Virtual server/ CPU：vCPU 4 /Memory：24 GB
Network：2 * 10Gbps /Disk space：250 GB/ OS：Windows 2016 or Linux

Air Gap Media Agent Server/ Virtual server /CPU：vCPU 8 ~ 12
/Memory：32 GB ~ 64GB /Network：1 * 10Gbps /Disk space：250 GB
/Backup Index：Depends on data capacity (500Gb to 2TB)
/DDB：Depends on data capacity (500Gb to 2TB)
/OS：Windows 2016 or Linux