TrustView®
Advanced Solutions for DLP

阻擋勒索軟體 & APT攻擊資料
隱形防護罩

匿蹤隔離保護機制為您守護

最具深度的自主防護，讓檔案隱形消失
在勒索軟體及APT攻擊竊取資料的威脅中

(02)2772-9900 | mkt@trustview.com.tw | 台北市復興南路一段205號5樓

匿蹤防駭客竊取，隔離破勒索攻擊

層出不窮的勒索軟體變種病毒，防不勝防，連 FBI 都建議付款了事。資安專家認為從「虛擬實體隔離」著手，是最有效阻絕未知的勒索軟體攻擊重要資料的方案，也是優先要導入的保護措施。

Wakanda

利用「匿蹤虛擬隔離技術」專注保護公司核心的資料，將資料庫(Database)、NAS站台或個人電腦中重要資料設定為「匿蹤隔離區」防護，在不影響ERP、CRM等系統作業下，隔離封鎖外部入侵的勒索軟體 / APT攻擊，避免重要資料被竊取及加密破壞

Scenario Wakanda 做核心資料的最後一哩保護

01. 保護MS SQL資料庫核心資料

Wakanda於伺服器站台上建置「匿蹤隔離區」機制，直接將資料庫檔案存放位置設定為隔離區，在不影響系統存取作業下，即可達到防護效果。

02. 保護檔案伺服器及NAS上的檔案

將檔案伺服器及NAS站台納入「匿蹤隔離區」內，只准許擁有通行證(Passport)使用者，經檢核安全後可存取檔案伺服器及NAS上的資料。

03. 保護個人電腦上的重要檔案

只要一個按鍵，就可直接將需要保護的資料夾設定為「匿蹤隔離區」，保護個人電腦上核心資料不受勒索軟體的威脅及破壞。

Solution Wakanda 自主防禦未知的勒索軟體及APT資料竊取

01. 保護區可控式安全程序清單

可設定匿蹤隔離區內可執行之應用程式及軟體，勒索軟體及惡意程式也無法於隔離區內執行。

02. 匿蹤虛擬隔離區

針對隔離區採取網路層及驅動層虛擬實體隔離技術，勒索軟體及駭客無法於安全隔離區外，利用網路或系統漏洞至受虛擬隔離保護的伺服器站台或資料夾。