SecureAge

SecureData

提供最大的資料保護

資料使用中

資料移動中

資料靜止中

內置於每個檔案的終極防護

SecureData 是什麼?

檔案 & 資料夾自動加密

SecureData 是一種具備智能、高靈活性、以策略模式運作基底和點對點的資料加密解決方案，不受任何儲存介質型態的限制，保護使用者資料檔案和資料夾資料外洩的風險.

獨特的 3P 技術集合專有的應用程式白名單和應用程式連結，不但能夠確保您的資料保持在被保護的狀態，同時也能夠抵禦漸進式持續攻擊威脅 (APT)、窺視攻擊以及中間人的攻擊行為.

Proactive

使用者無需要有意識地一直記得必須要對系統正在處理的資料加密，能夠確保自然工作流程的安全性.

Pervasive

無論的檔案是停駐在您系統任何地方，每一個檔案都是加密的 – 從檔案建立到儲存於任何地點或是任何媒介，甚至是雲端.

Persistent

每一個檔案在網路傳輸流通的過程中都是保持加密狀態，從而使其免於網路偷窺攻擊和中間人攻擊.

3P 技術

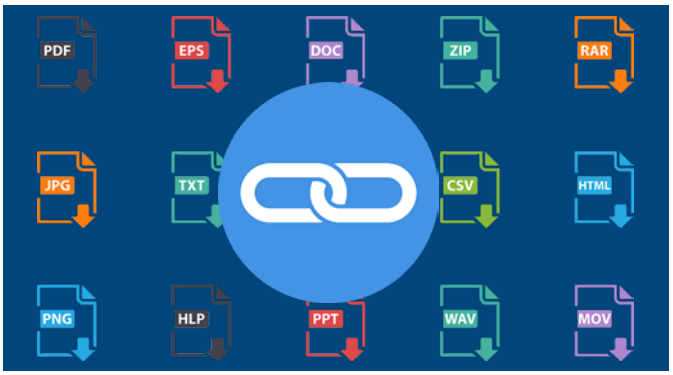
SecureData 的基本原則是提供任何資料檔案的透通性加密，無論資料檔案是在靜止狀態、傳輸過程中或是存在於任何儲存系統，資料檔案都是處於加密狀態，能夠避免任何人在網路進行偷窺攻擊, 並且獲取任何有用的資訊.

應用程式白名單

針對處理複雜的漸進式持續攻擊威脅 (APT) 和惡意軟體所設計，包含了應用程式白名單組件, 能夠智慧巧妙地建立一個信任且允許運行的應用程式完整名單.

能夠有效地封鎖所有新的可執行的惡意軟體運行，並且使已存在的現有惡意軟體無法再進一步去感染其他的電腦.

應用程式連結



確保只有特定和授權的應用程式能夠存取資料, 以保護機密敏感資料免於遭受零日攻擊惡意軟體潛在的進程攻擊.

應用程式連結能夠限制例如瀏覽器等高風險的應用程式, 在未經使用者同意的情況下自動存取敏感機密資料, 建立一個“應用程式沙盒”，讓只有特定目錄的檔案具備讀寫功能.

主要優勢 & 技術

資料隱私並不會影響工作效率

只需要終端使用者有最低程度的培訓以確保日常資料使用安全的落實. SecureData 具有的功能不但不會削弱生產力，還能夠在抵禦內部和外部攻擊的同時發揮生產力.

- 隨時隨地將所有檔案自動加密，包含臨時 & 系統頁面檔案.
- 能夠針對網路資料流量進行完整的加密 (亦即網路伺服器 & 磁碟).
- 對於檔案建立、編輯 & 複製/移動到任何存儲裝置採取一站式的加密.
- 支援多個 & 同步智慧卡、USB 以及 HSM.

明確的落實

整合 SecureData 和各種不同的系統應用程式僅需要極少的人力花費,，並由專門的支援小組提供專業知識進行協助.

- 提供易於配置的策略控制，以支援企業安全的需求.
- 提供使用者特定的策略控制，為不同的使用者提供不同的安全權限.
- 透過 web 控制台進行集中策略更新和日誌管理.
- 支援全面性的金鑰管理.

軍事等級的安全功能

SecureData 是專門為滿足軍事資訊安全標準而打造, 結合了關鍵技術並提供了無與倫比的資料保護.

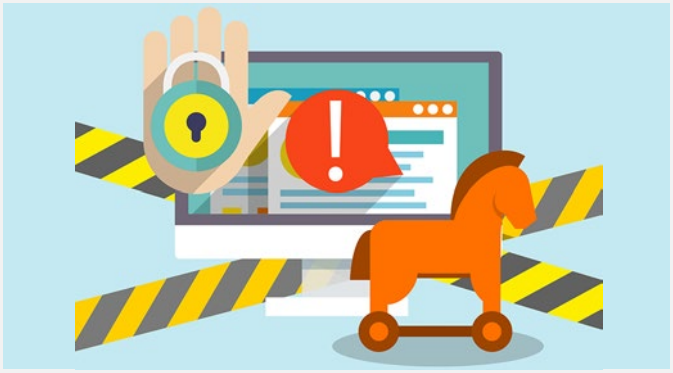
- 專為進階使用者提供預設 256-bit AES 加密 & Elliptic Curve Cryptography (ECC)
- 無限金鑰長度 RSA & DSA
- 提供無限使用者金鑰歷史紀錄支援和多使用者設定檔管理
- 可客製化加密演算法
- 使用對等憑證本地管理進行 PKI 優化
- 雙向身分認證的 TLS/SSL 連線
- 支援標準 X.509 v3 憑證

符合全球安全法規規範

輕鬆達成全世界最挑剔的資訊立法的法規規範. SecureData 符合下列規範:

- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Sensitive Agency Info (White House OMB)
- Sarbanes-Oxley (SOX)
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Monetary Authority of Singapore Technology Risk Management (TRM)
- Various Data Breach Disclosure Bills (i.e. California SB 1386, European E-Privacy Directive)

SecureData 戰略上的重要應用程式



APT 防制 & 惡意軟體防制

SecureData 的惡意軟體防制組件結合應用程式 & 資料控制 (專利) 的解決方案，能夠檢測、阻止和刪除已知的威脅，例如 rootkit、間諜軟體、病毒、特洛伊木馬和其他惡意程式碼，同時保護使用者端免於遭受 APT 的攻擊.

應用程式白名單組件能夠確保任何被攻擊者竊取的資料，仍然會保持在加密的狀態，讓被竊取的資料無所作用. 另一方面，應用程式連結透過自動限制高風險應用程式的模式，在沒有使用者的同意之下，無法去存取資料檔案，大大降低了零日攻擊的風險.

針對企業伺服器

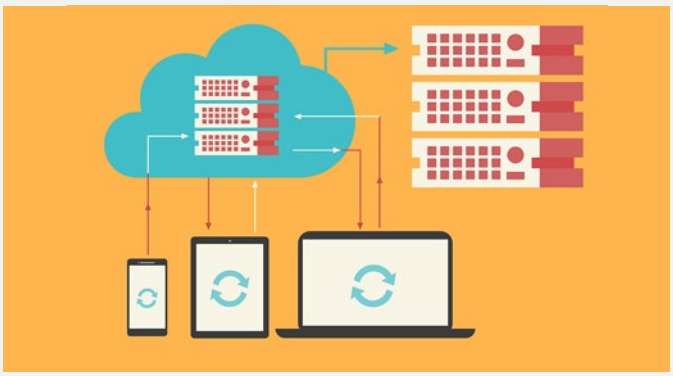
企業組織保護機密敏感資料會獨自將資料儲存在檔案伺服器、企業資料庫、Microsoft SharePoint、企業專有的特殊應用程式伺服器、FTP 伺服器和備份磁帶上. 儲存在伺服器中的任何資料，不論資料在伺服器和使用者端的電腦間移動，資料都會保持在加密的狀態.

透過授權使用者自己專屬的金鑰對機密敏感資料加密的限制，能夠進一步增強企業伺服器的安全性. 如此，即使具有管理員權限的未經授權使用者，也無成功地進行內部攻擊.

針對資料庫伺服器

SecureData 使用檔案等級的加密，能夠自動對資料庫內結構化的資料以及資料庫外非結構化的資料加密. 與列級加密和 Transparent Data Encryption (TDE) 不同，整個資料庫是被加密的，同時也能夠透過 all-in-one 的解決方案將營運成本降到最低.

由於加密過程對資料庫和應用程式是通透的，因此資料在加密時並不需要對現有資料庫和應用程式做任何的更改. 能夠大大提高資料庫安全性的操作效率.



針對雲端計算

SecureData 對於機密敏感性資料以不可思議且靈活性的統一策略，進行配置和實施保護措施，允許不論資料是儲存在任何地方，都能確保資料始終是處於加密的狀態. 這顯示任何儲存在使用者端電腦以外的資料，尤其是在雲端伺服器上的資料，更能夠確保資料的完美安全.

任何試圖竊取機密敏感資料，不論是來自雲端運雲商內部和外部參與的雲端管理員，沒有使用者的加密金鑰解密，都只夠拿到加密的資料而已.

需要更多的資訊嗎?

www.secureage.com contactus.tw@secureage.com