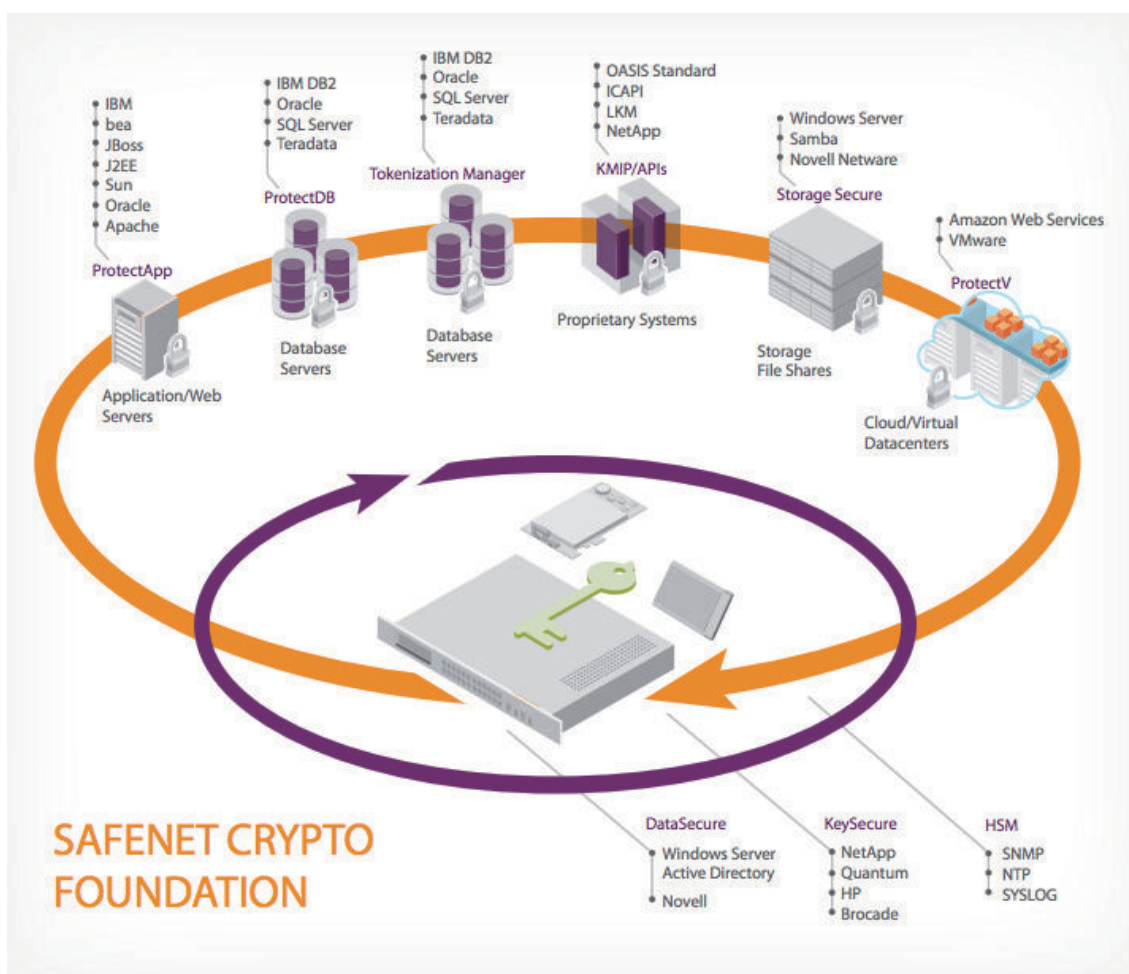


# SafeNet 金鑰管理安控模組設備解決方案

撰文：叡揚資訊 資訊安全事業處

SafeNet DataSecure 提供使用者對應用系統、資料庫、檔案及虛擬主機加解密之功能，可細膩的整合集中金鑰管理的功能，從而提供點對點、簡易且高成本效率的加密解決方案。透過其在網路伺服器、應用伺服器、資料庫伺服器、檔案系統與分散式環境下對機敏資訊執行加密功能。DataSecure 可以協助企業保護可能導致業務風險的機敏資料—不論是信用卡卡號，個人身分證號碼或是其他任何機敏資訊。

其中 SafeNet DataSecure i460 型號中內嵌 SafeNet Luna HSM 卡，符合 FIPS140-2 Level 3 標準。DataSecure 可於單一設備裝置上集中所有加密處理技術、金鑰管理、紀錄與稽核、資安管理準則；因此，可協助建置大規模全面化之資安基礎建設，在商業化解決方案之中提供最高等級的資安保護。



## SafeNet 重要特色：

1. DataSecure 內建的密碼系統可以加密或解密資料，建立 MAC，建立數字簽名，並提供亂數產生器。內建密碼系統提供以下各公眾演算法：

- ◆ AES
- ◆ ARIA
- ◆ DES
- ◆ 3DES
- ◆ HMAC-SHA1
- ◆ HMAC-SHA256
- ◆ HMAC-SHA384
- ◆ HMAC-SHA512
- ◆ MD5
- ◆ RC4
- ◆ RSA
- ◆ SEED

其中各對稱式演算法中均支援 ECB、CBC 模式，非對稱式密碼演算法中 RSA 長度可達 4096 bits。

2. DataSecure 將所有加密處理與管理機制集於一身，具有強健性能，滿足任何環境及高度專業化之加密作業。透過啟動負載平衡功能，可以非常容易將工作量分配至增加的 DataSecure 設備，達到擴充效能的需求；同時簡化加密操作，另外亦可達到降低伺服器（包含應用系統、檔案及資料庫伺服器）CPU 密集加密之工作負載，提高該伺服器之處理效能，DataSecure 將伺服器與資料庫的效能提昇到最佳等級，實現較短資訊等候時間與較高資源利用率。

3. DataSecure 採用了高速硬體的加密方式，涵蓋最廣泛的資料類型。

4. DataSecure 具有彈性的參數設定，便於企業選擇適當的資料處理和安全等級，滿足當前和未來的需求。部署 DataSecure 設備後，可以在軟體安全保護選項中，選擇資料中心和終端資料保護方式。使用 DataSecure 可以針對企業特定的需求提供量身訂做式的解決方案。