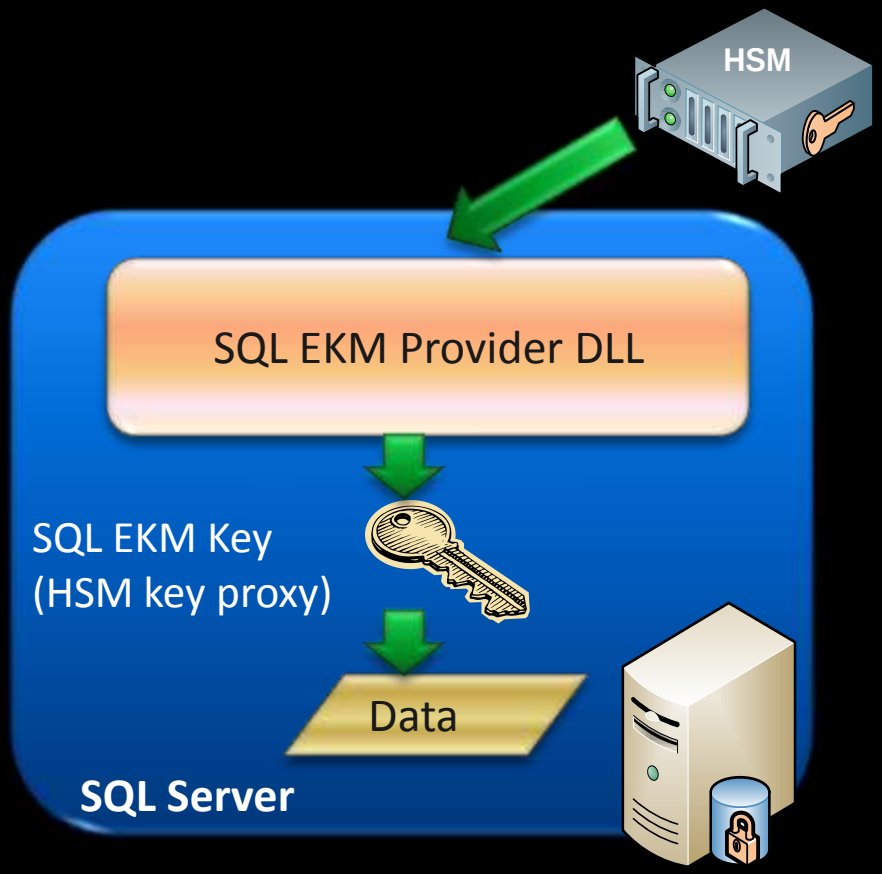
創新的防禦術
SQL SERVER 2008

資料加密

- 資料加密
  - 透過密碼、加密金鑰等方式讓資料變成模糊無法識別
  - 讓具備管理權限的人員或是入侵的駭客，也無從得知資料的原貌
  - 早期的資料加密作業
    - 多半是由前端應用程式自行控制
    - 需要使用大量的 CPU資源
    - 加密金鑰與加密資料一起存放
- SQL Server 2005
  - 內建：密碼片語、對稱金鑰、非對稱、憑證的加密功能
  - 使用 SQL Server 作為金鑰管理
  - 加密檔案系統 (Encrypted File System，EFS)
  - BitLocker 磁碟加密功能
- SQL Server 2008
  - 可延伸金鑰管理(Extensible Key Management，EKM)
  - 透明資料加密(Transparent Data Encryption，TDE)

可延伸金鑰管理 (EKM)



- 使用「硬體安全性模組」(Hardware Security Modules，HSM)
- 廠商可以對 HSM、金鑰組態和金鑰存取提供管理軟體 -- MSCAPI提供者
- SQL EKM金鑰提供代理功能來存取HSM金鑰
- 讓 SQL Server 可以使用由協力廠商所開發的模組元件，支援進階加密功能和金鑰管理函數

EKM的特性

- 優點
  - 安全性
    - 外部加密金鑰儲存 (實體分隔資料和金鑰)
    - 企業能中央管理與儲存金鑰機制
    - 額外的授權檢查 (啟用責任分隔)
    - 分隔資料庫擁有者(db_owner)與資料擁有者(data owner)
  - 效能
    - 硬體架構加密/解密的效能高
- 限制
  - 適用 Enterprise版本

EKM密碼編譯提供者與金鑰

- EKM提供伺服器層級物件

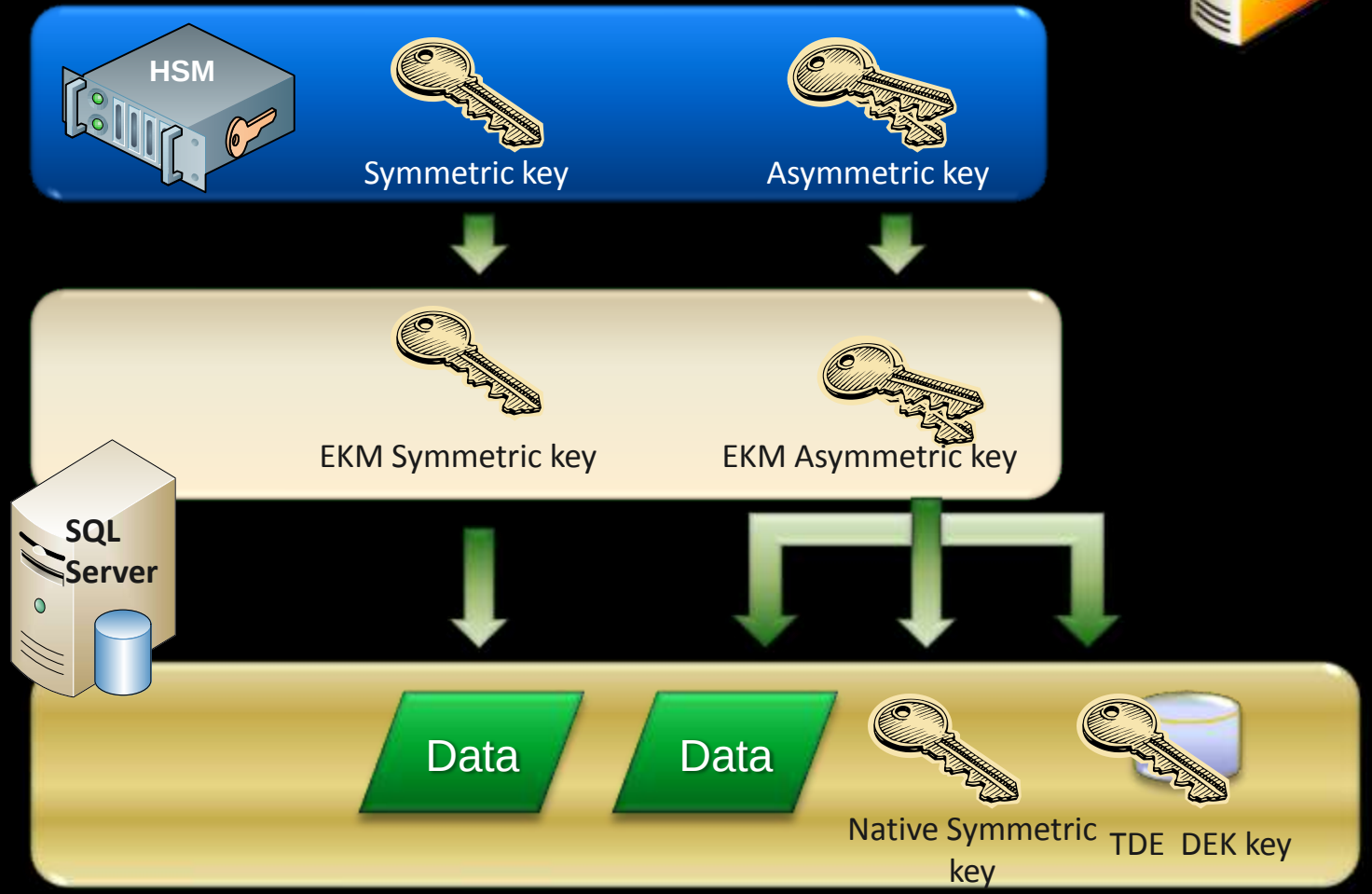
```
CREATE CRYPTOGRAPHIC PROVIDER DataSafeProvider
FROM FILE = 'DataSafeProvider.dll'
```

- 使用EKM的金鑰
  - 管理-相同的T-SQL

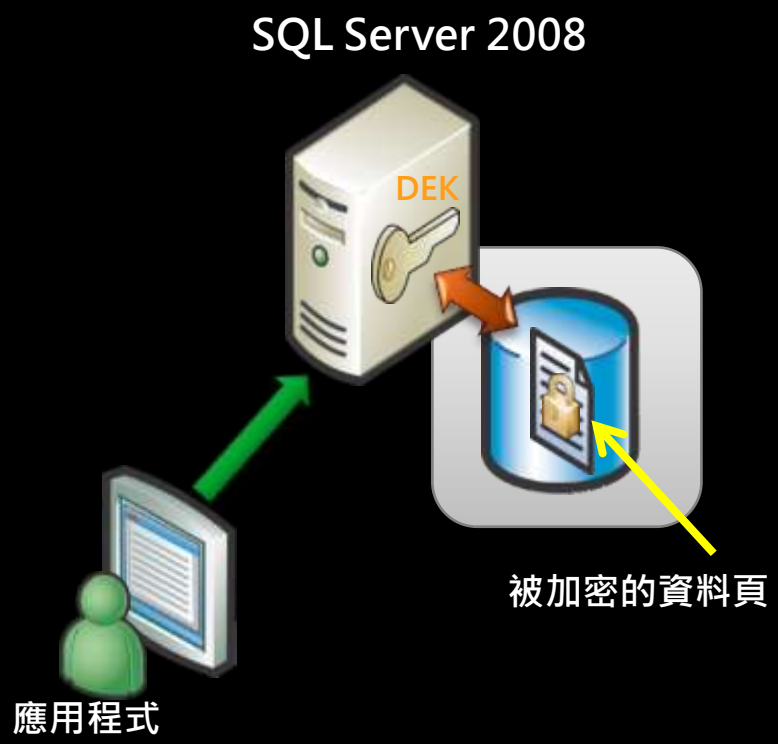
```
CREATE SYMMETRIC KEY SymmKeyEkm
FROM Provider DataSafeProvider
WITH ALGORITHM AES_256 …
```

  - 使用-相同的T-SQL
    - 檢視金鑰資訊、資料的加解密等
    - EncryptByKey、DecryptByKey、EncryptByAsmKey、DecryptByAsmKey 等

EKM 金鑰的階層結構


HSM
Symmetric key
Asymmetric key
EKM Symmetric key
EKM Asymmetric key
SQL Server
Data
Data
Native Symmetric key
TDE DEK key

透明資料加密(TDE)



- 無需修改應用程式
- 在資料庫層級：加密與解密
  - 使用資料庫加密金鑰 (DEK)
- DEK 使用以下的方法來保護
  - 憑證
  - 硬體安全性模組(HSM)
- 必須有DEK
  - 還原資料庫
  - 附加資料庫檔案

TDE-加密金鑰階層

- 加密資料
  - 選用 AES 或是 3DES加密演
  - 雖然會增加 CPU使用量，
    不會增加資料庫的使用空
  - 執行資料庫備份作業時，
- 運作原理
  - 先對存放在記憶體的資料
    寫入到磁碟上。
  - 完成加密後，使用總和檢
    護機制。
  - 需要解密的分頁載入記憶
    查碼，事先即可偵測分頁
  - 資料分頁進行解密，再載

使用 TDE 的理由

- 保護機密資料(data at rest)
- 整個資料庫受到防護
- 應用程式無需修改
  - 索引或資料類型也沒限制(但不支援 FileStream)
- 對於效能衝擊很小
- 備份時無需使用金鑰

TDE 使用情境

阻斷使用者直接存取資料庫的檔案系統

防禦未經授權的使用者取得資料庫備份檔案

符合規範：保護機密的靜態資料(data at rest)

沒有使用憑證或HSM解開金鑰，將無法開啟資料庫

使用 TDE 的考量

- 可與資料壓縮一併使用
- 不建議與備份壓縮一併使用
- 資料庫鏡像
  - 複製憑證到主體與鏡像伺服器上
- 將虛擬記錄檔案 (virtual log file) 內的其餘部分設為零，以強制使用下一個虛擬記錄檔案
  - 無法使用立即檔案初始化(instant file initialization)，對於復原資料庫、取得磁碟空間，有負面影響
- 一旦某一資料庫使用 TDE
  - tempdb 系統資料庫也將加密，這對於未啟用 TDE 的資料庫將會有效能的影響
- 適用 Enterprise版本