
CYBERSEC 2022 臺灣資安大會
CHANGE NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

資料庫安全防護 —
金鑰管理、加密、代碼化

亞利安科技 技術部協理
王添龍

CipherTech
TRUST&SECURITY

Thales Accelerate
Partner Network
PLATINUM

資料庫是企業重要資產

過去著重在網路架構、存取控制層面考量資料庫安全，雲端應用的出現使得**資料本身的安全**受到重視。

個資法施行已將近10年，期間科技的演進、駭客手法的創新、高權限帳號的控管問題歷歷在目…

企業內部最珍貴的資產在於**資料**，許多內部系統都使用**資料庫**儲存及管理資料。

資料保護好了嗎?

影響我們的主要資安趨勢是什麼?

資料洩露正以前所未有的速度增加當中

- 資料遭竊通常是肇因於一連串的防禦漏洞
- 許多資料庫遭受攻擊是因為錯誤的設定與權限控管疏漏
- 數據開放與大量使用API及套件, 產生新的存取途徑

將資料遷移到雲端可以使公司更加敏捷，但缺乏安全性會使他們更容易受到攻擊

資料的數量和多樣性意味著組織甚至看不到他們需要保護的內容

- 檔案、各個營運系統、SQL、NoSQL、VM、雲端、大數據、Container、舊系統..

保護數據是一項艱鉅的工作，公司通常擁有來自 40 家供應商的 80 種工具來嘗試解決問題

- 要做的事很多、廠商多、工具更多..

資安健診服務(1/2)

大項	大項標題	中項標題	服務項目	小項標題	檢視項目	內容說明
8	資料庫安全檢視	8.3	存取授權	8.3.11	限制資料庫主機服務埠	· 訪談資料庫主機連線對象、連線目的及使用之服務埠 · 實機檢視資料庫主機僅開啟允許之服務埠
8	資料庫安全檢視	8.3	存取授權	8.3.12	限制遠端存取來源	· 訪談資料庫遠端存取控管機制 · 檢視資料庫遠端存取來源、連線授權紀錄，避免遭非授權來源IP進行連線
8	資料庫安全檢視	8.3	存取授權	8.3.13	限制遠端存取帳號	· 檢視資料庫遠端存取帳號與授權紀錄，避免遭非授權帳號進行遠端存取
8	資料庫安全檢視	8.3	存取授權	8.3.14	限制遠端存取操作	· 檢視資料庫遠端存取權限與授權紀錄，避免執行非授權之操作行為
8	資料庫安全檢視	8.3	存取授權	8.3.15	資料庫帳號權限最小原則	· 訪談資料庫身分識別、存取管理及權限劃分機制 · 檢視資料庫權限相關申請、審核紀錄，並實機檢視資料庫帳號權限遵循最小化原則
8	資料庫安全檢視	8.4	稽核紀錄	8.4.16	啟用資料庫帳號變更稽核	· 訪談資料庫稽核紀錄留存項目、保存期間及管理機制 · 實機檢視資料庫帳號異動稽核紀錄設定結果、留存內容及管理方式
8	資料庫安全檢視	8.4	稽核紀錄	8.4.17	啟用資料庫帳號登出/登入稽核	· 實機檢視資料庫帳號登入/登出稽核紀錄設定結果、留存內容及管理方式
8	資料庫安全檢視	8.4	稽核紀錄	8.4.18	啟用資料庫結構變更稽核	· 實機檢視資料庫結構異動稽核紀錄設定結果、留存內容及管理方式
8	資料庫安全檢視	8.4	稽核紀錄	8.4.19	稽核紀錄管理方式	· 檢視資料庫稽核紀錄之存取控制與保存紀錄
8	資料庫安全檢視	8.4	稽核紀錄	8.4.20	資料庫主機時間校時	· 訪談資料庫主機校時管理機制 · 實機檢視資料庫主機校時方式、來源及時間正確性
8	資料庫安全檢視	8.4	稽核紀錄	8.4.21	稽核紀錄分析	· 訪談資料庫稽核紀錄分析機制及異常紀錄處理方式 · 實際檢視資料庫稽核紀錄分析規則設定、分析紀錄或報告，以及針對異常事件處理方式

資安健診服務(2/2)

資料加密列入服務項目中

大項	大項標題	中項標題	服務項目	小項標題	檢視項目	內容說明
8	資料庫安全檢視	8.2	資料加密	8.2.8	資料庫資料具有適當保護機制(包含加密、去識別處理)	· 訪談資料庫資料保護機制(如加密方式、保護資料範圍、不可識別處理之方式等) · 實機檢視資料庫資料之加密設定、加密結果、不可識別處理之結果
8	資料庫安全檢視	8.2	資料加密	8.2.9	資料庫資料具有安全傳輸機制	· 訪談資料庫傳輸保護機制 · 實機檢視資料庫資料傳輸加密方式與設定狀況，避免採用不安全的資料傳輸方式
8	資料庫安全檢視	8.2	資料加密	8.2.10	資料庫加密金鑰需具有適當保護機制	· 談資料庫加密金鑰管理機制(如使用狀況、保管情形等) · 檢視資料庫金鑰存取相關申請、審核紀錄及金鑰管理方式，避免遭非授權人員存取

資安法中有關加密的規定(1/3)

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。		一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取

39

			機關內部網段或資通系統後臺之連線。 四、應採用加密機制。

存取控制 – 遠端存取：

等級高、中、普均應採用加密機制

資安法中有關加密的規定(2/3)

系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證應定期更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防	無要求。	無要求。

43

		護措施。		
	資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。

系統與通訊保護 – 傳輸之機密性與完整性：
等級高的資通系統應採用加密機制,
加密金鑰或憑證應定期更換。

系統與通訊保護 – 資料儲存之安全：
等級高的資通系統重要組態設定檔案及
其他具保護需求之資訊應加密或以其他
適當方式儲存。(修正前僅規範靜置資料)

資安法中有關加密的規定(3/3)

			試登入或使用機關自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	

識別與鑑別– 加密模組鑑別：
等級高、中的資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。

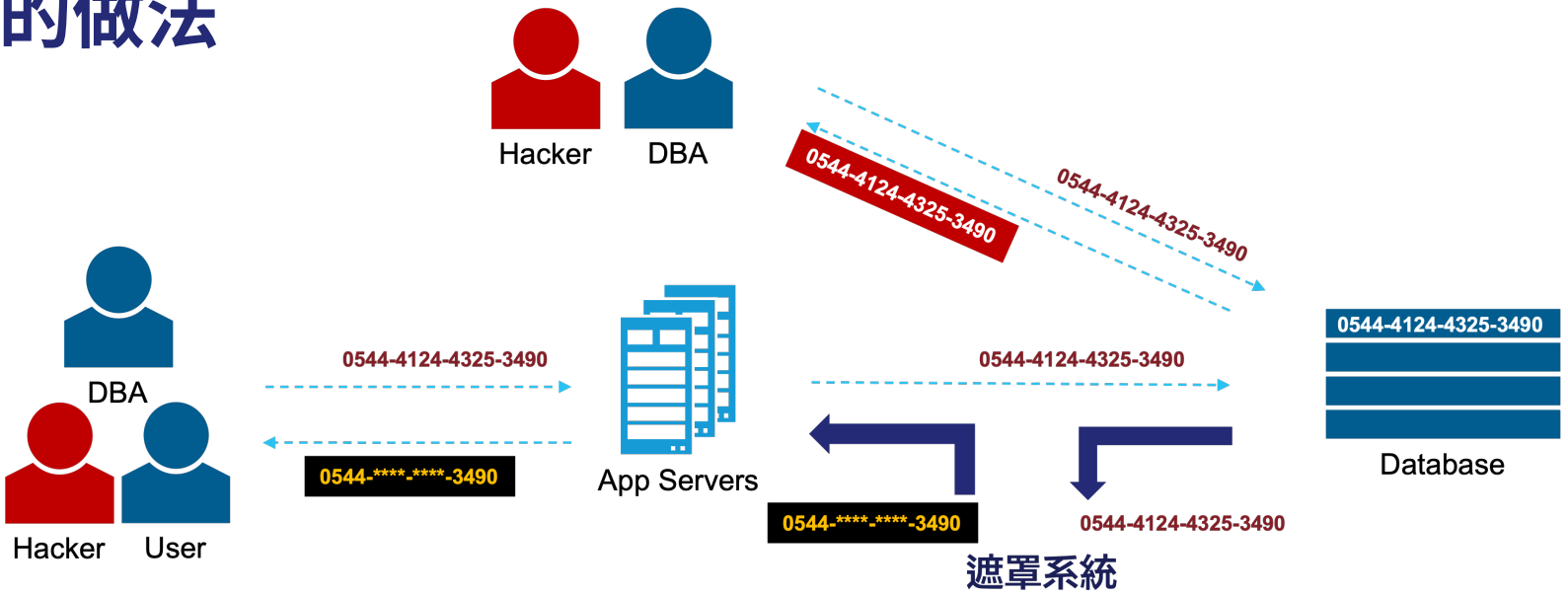
資安法中有關加密的規定(3/3)

- **具保護需求之資訊要加密**
  (資料庫、密碼、個資…)
- **傳輸過程要加密**
- **金鑰管理及適當保護**

保護資料庫的方式

遮罩	資料讀取過程中變造，使有權限的人才能看到完整資料，不改變在資料庫中的資料，若資料庫遭竊或利用非正規路徑存取，看到的都是明碼資料。無法符合法規對資料庫加密的要求。
稽核	留存資料使用軌跡，不變更資料，絕大多數用戶為的是留Log, 並不會啟用阻擋功能，因此無法有效阻止資料遭竊。
加密	寫入時將資料庫中的重要資料加密保存，讀取時判斷權限是否解密，即便資料庫被複製，也無法輕易獲取明碼資料。

遮罩的做法

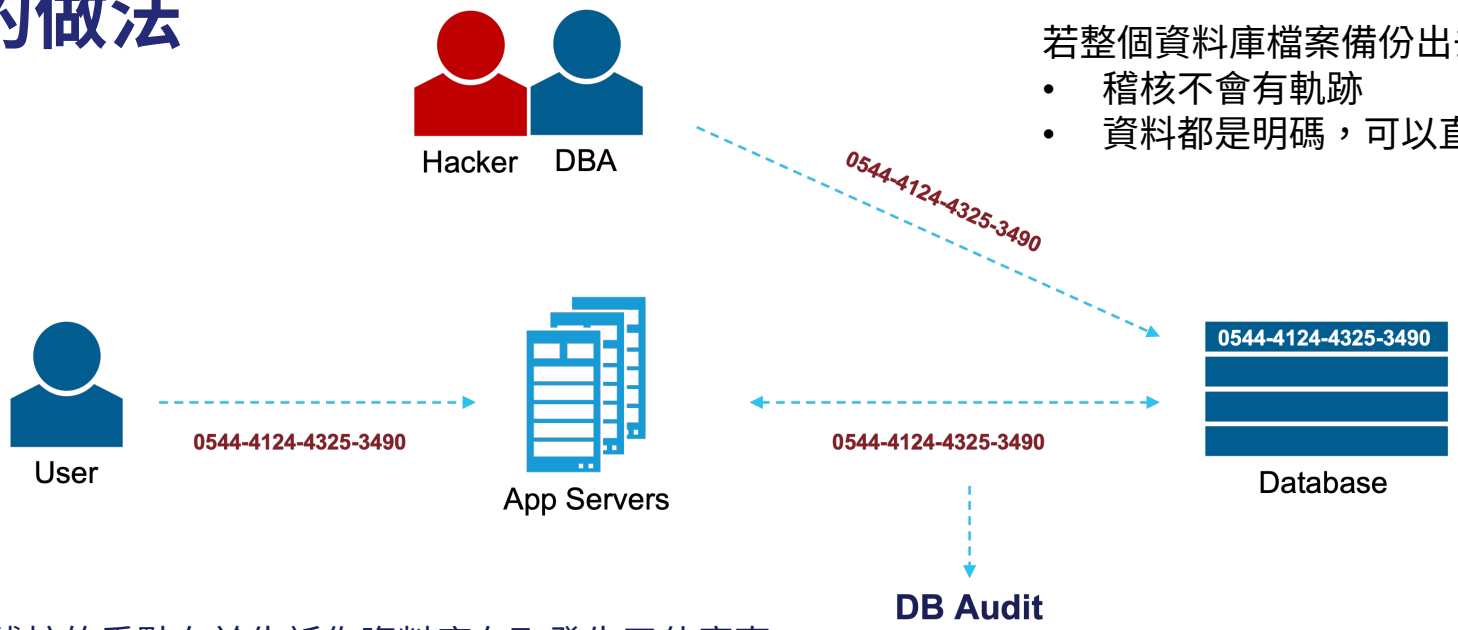


現今國內外法規、稽核員認為
此做法已經無法真正保護資料

讀取資料時，透過遮罩系統將資料依據Policy變造，
使前端程式或使用者只能看到部分資料。

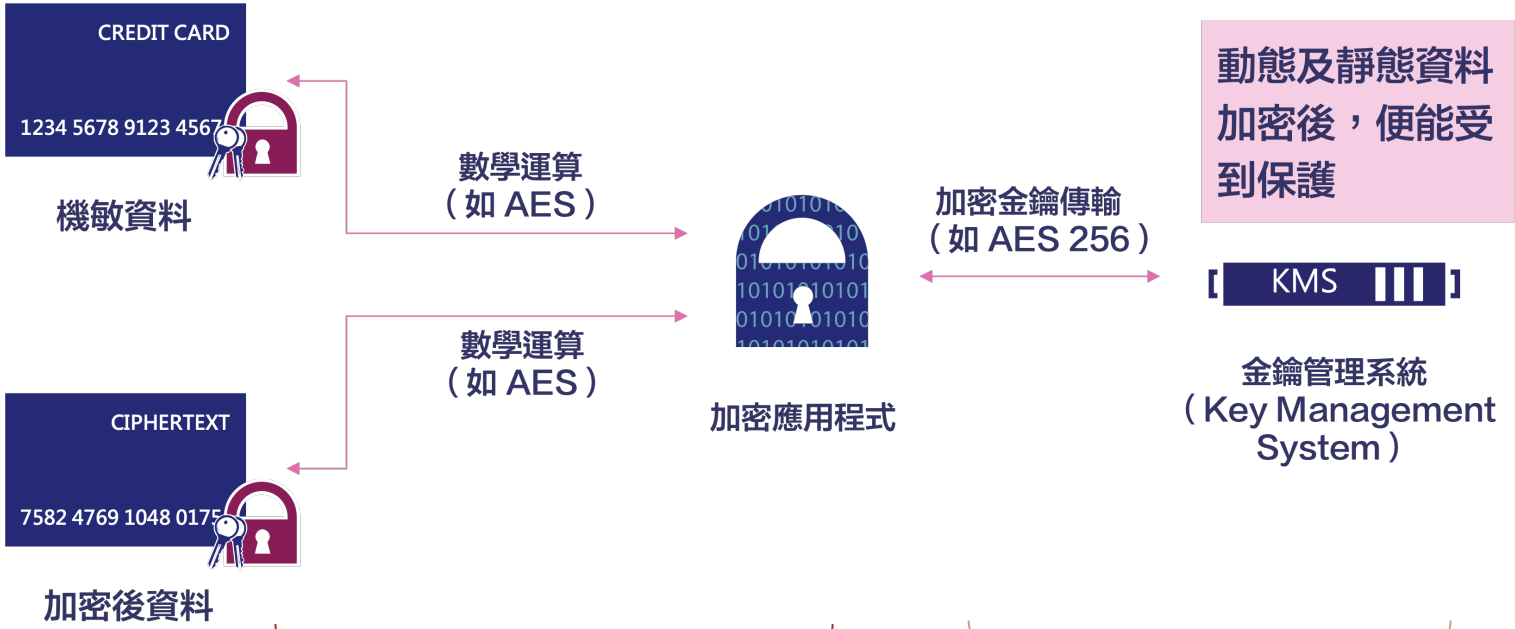
直接存取資料庫，可取得明碼完整資料
若整個資料庫備份出去，資料都是明碼，可以直接回復

稽核的做法



- 資料庫稽核的重點在於告訴你資料庫存取發生了什麼事
- 對異常行為能發出告警
- 若採用Inline架構或是靠本機Agent則可以阻擋

加密是保護資料最直接的方式



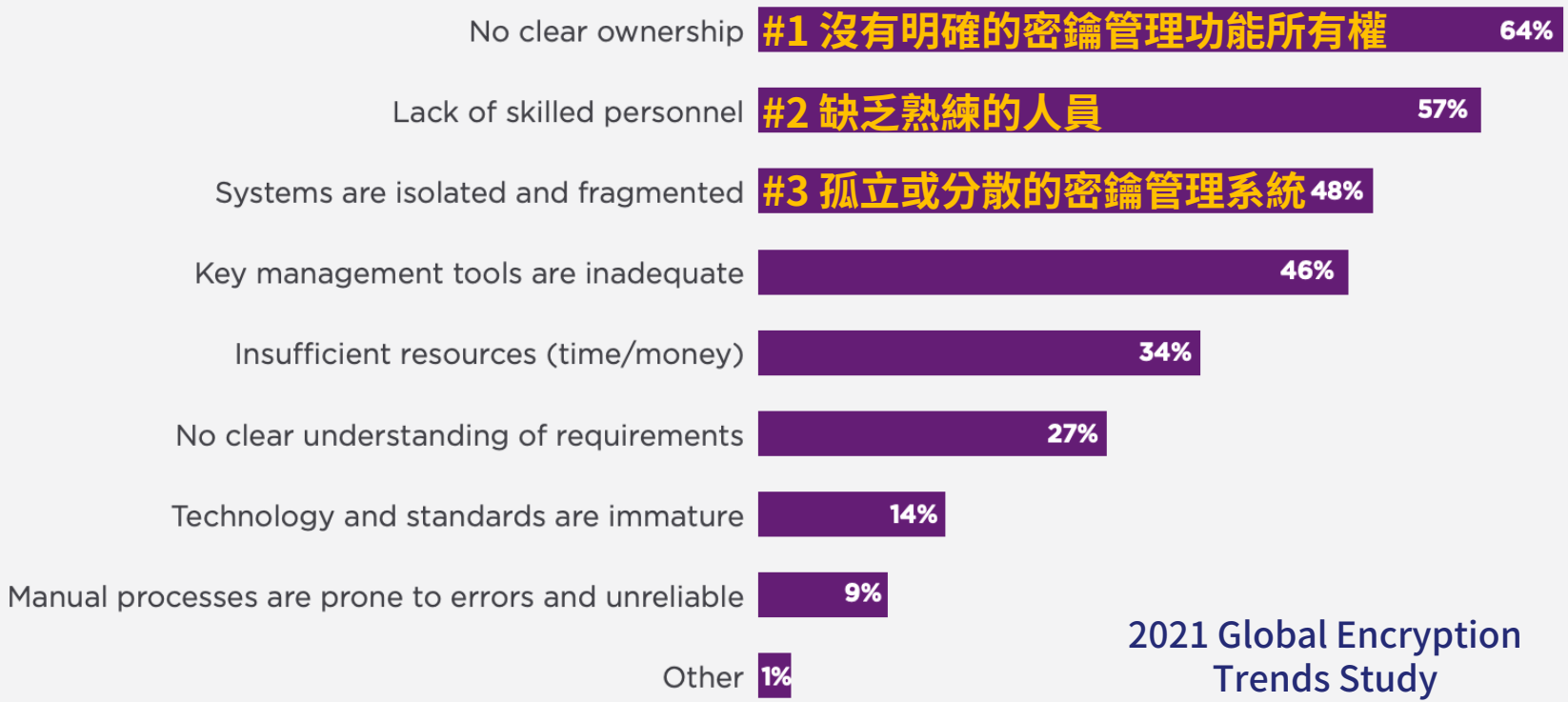
過往資料加密保護面臨的問題

效能

金鑰管理

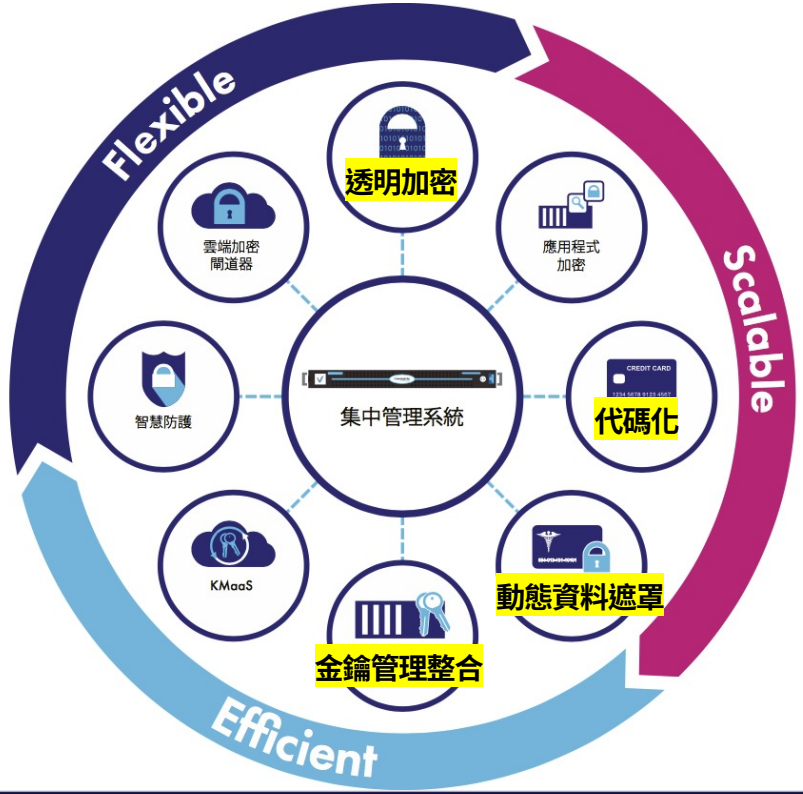
建置複雜度

金鑰管理的痛點



2021 Global Encryption Trends Study

Ciphertrust 資料保護平台



兼顧

- 佈建彈性
- 擴充性
- 效能

方案一、檔案加密

Security Intelligence
Logs to SIEM

Ciphertrust Manager
金鑰管理系統

Privileged Users

*$^!@#)(
-|"_}?$%-:>>

root SA

user

Approved Processes and Users

John Smith
401 Main
Street

Encrypted & Controlled

Clear Text

User

Application

Database

File Systems

Volume Managers

Storage

Server

Allow/Block
Encrypt/Decrypt

Cloud Admin, Storage Admin, etc

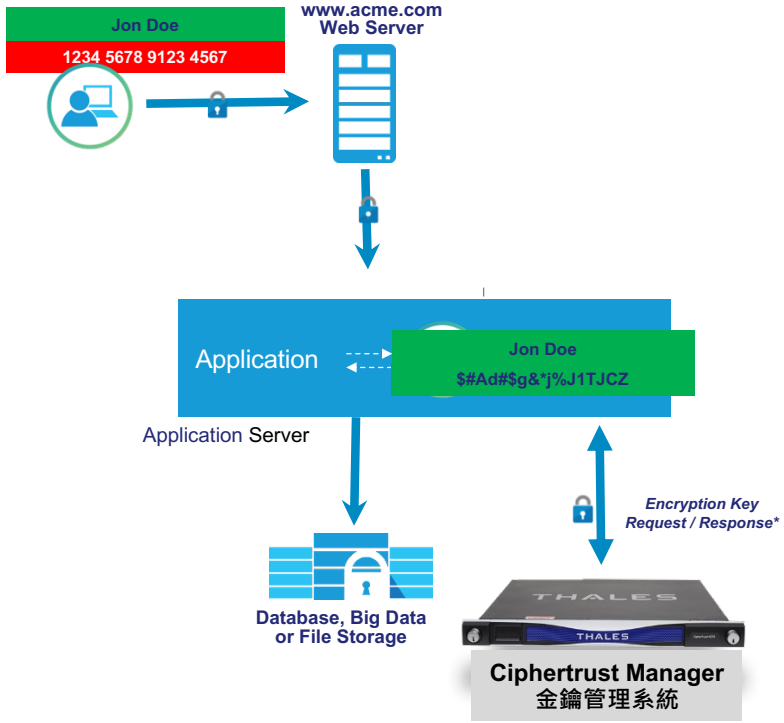
Encrypted

*$^!@#)(
-|"_}?$%-:>>

Big Data, Databases or Files

架構單純、佈建快速、不改變使用者操作方式

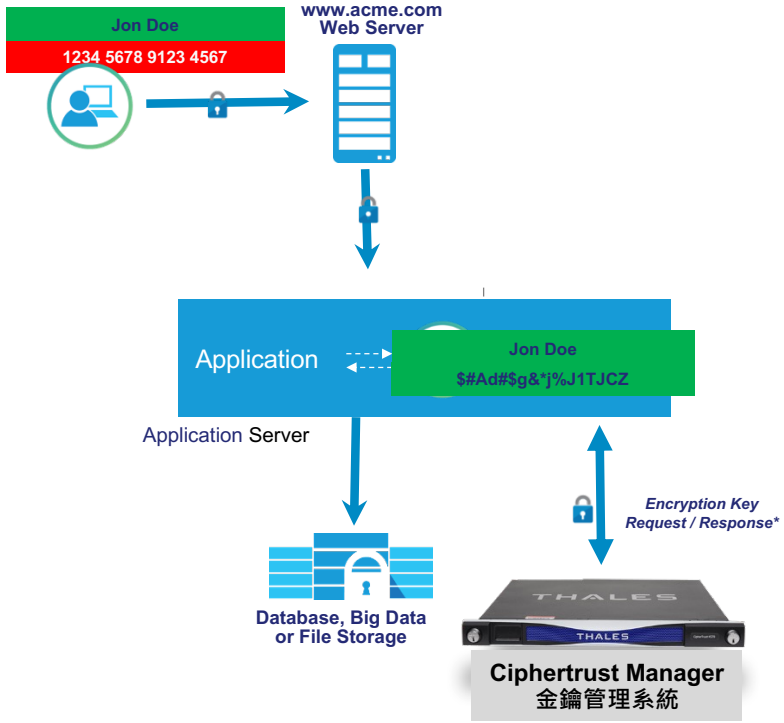
方案二、Tokenization



資料在應用程式處理時進行加密

- ✓ AP控制加密、解密
- ✓ 寫入資料庫前已經將資料加密
- ✓ 備份資料也是加密狀態

方案二、Tokenization



資料在應用程式處理時進行加密

- ✓ AP控制加密、解密
- ✓ 寫入資料庫前已經將資料加密
- ✓ 備份資料也是加密狀態

方案二、Tokenization

0544-4124-4325-3490

CipherTrust
Tokenization

4269-8572-9741-2570

機敏資料

代碼化

儲存受保護的資料

裝Agent – 怕影響效能?

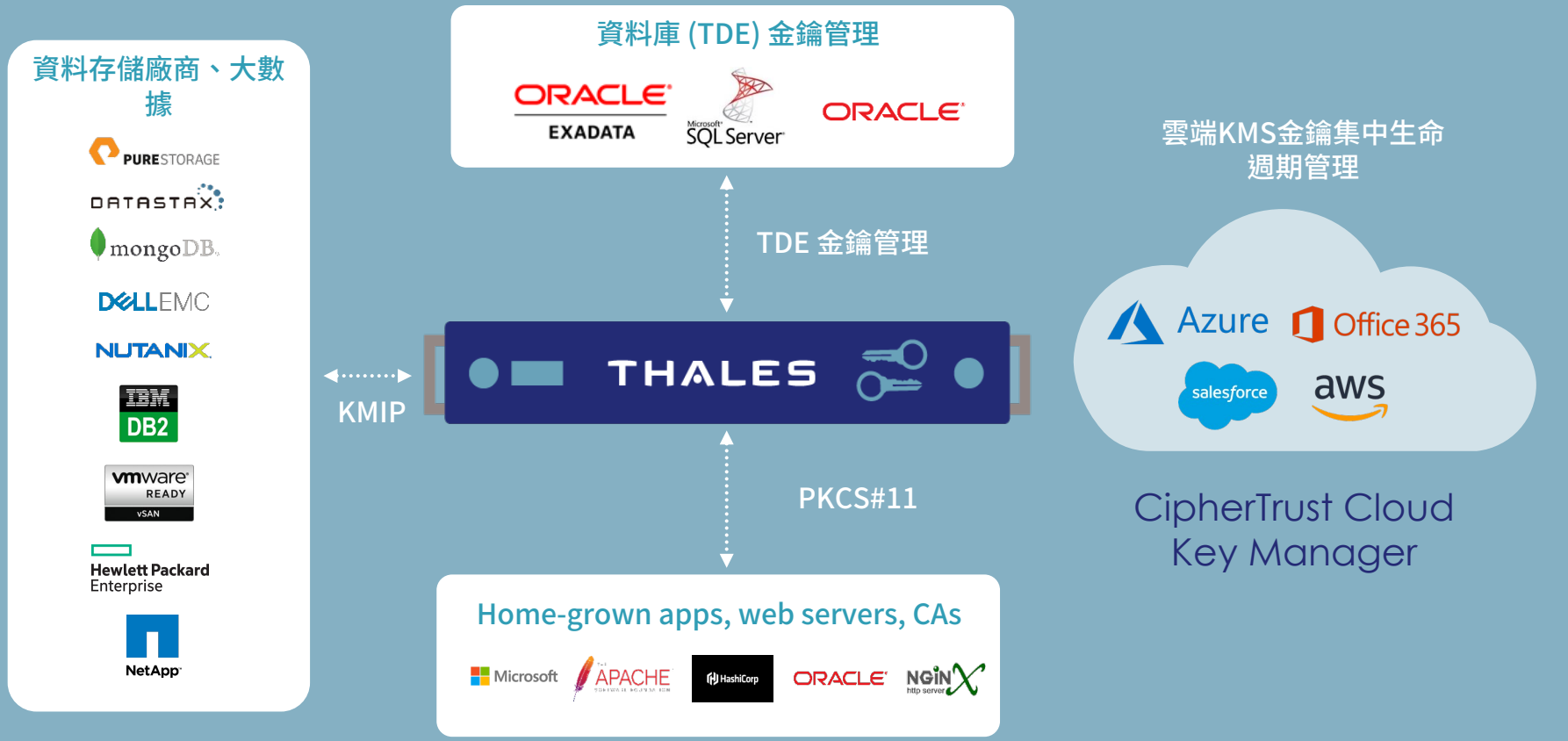
代碼化 – 改程式可能非常麻煩?

資料庫內建的加密機制是否可用???
（加密資料跟金鑰都一起放在資料庫中）

方案三、金鑰整合

廣泛多樣的整合

支援最多數量的KMIP應用


資料存儲廠商、大數據
PURESTORAGE
DATASTAX
mongoDB.
DELL EMC
NUTANIX
IBM DB2
vmware READY vSAN
Hewlett Packard Enterprise
NetApp
資料庫 (TDE) 金鑰管理
ORACLE EXADATA
Microsoft SQL Server
ORACLE
TDE 金鑰管理
KMIP
THALES
PKCS#11
Home-grown apps, web servers, CAs
Microsoft
APACHE
HashiCorp
ORACLE
NGINX http server
雲端KMS金鑰集中生命週期管理
Azure
Office 365
salesforce
aws
CipherTrust Cloud Key Manager

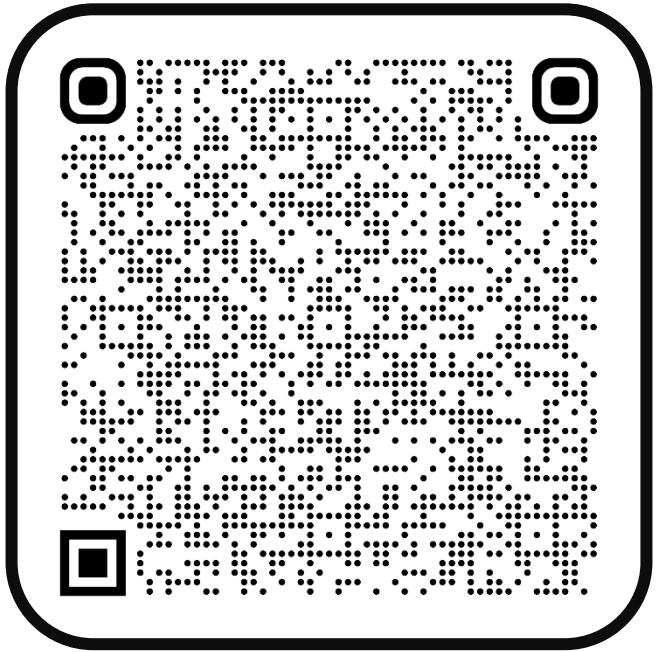
根據需求在您需要的地方提供資料安全保護

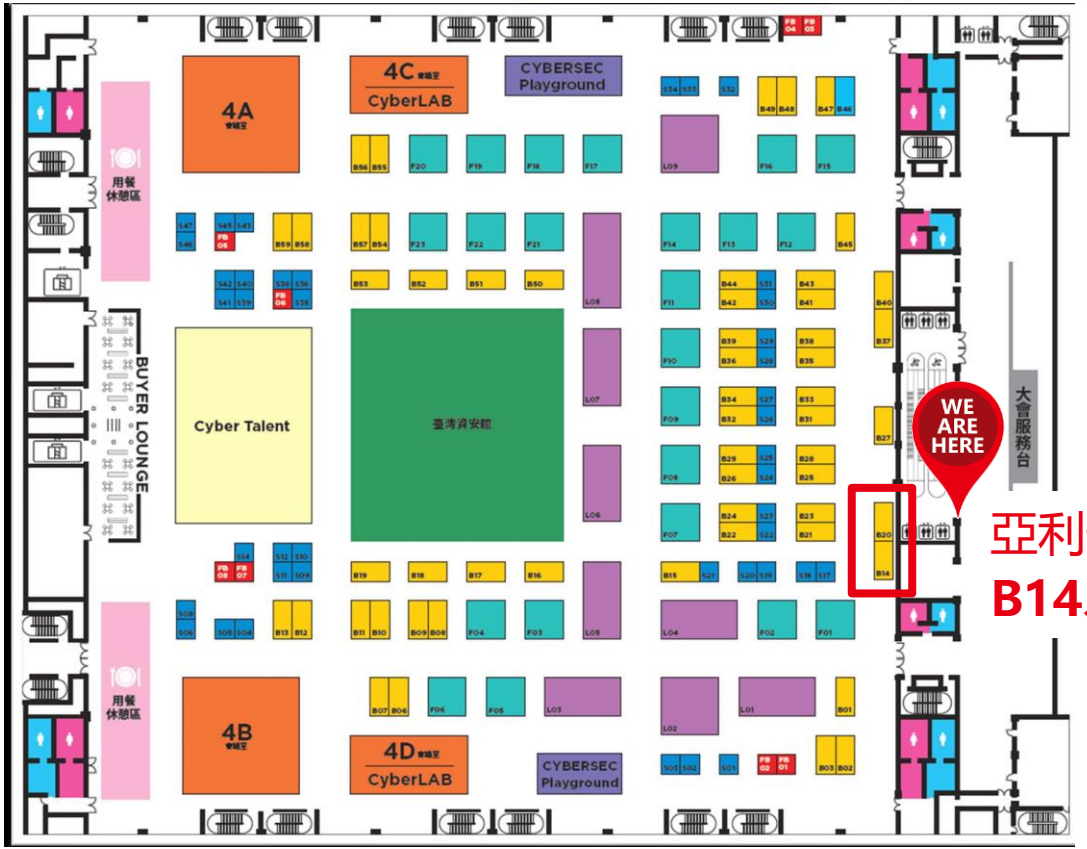
CipherTech
TRUST&SECURITY

Thales Accelerate
Partner Network
PLATINUM

邀請您填寫線上問卷，讓我們更了解您的需求

填寫完畢，即可兌換品牌好禮！





亞利安科技
B14、B20 攤位