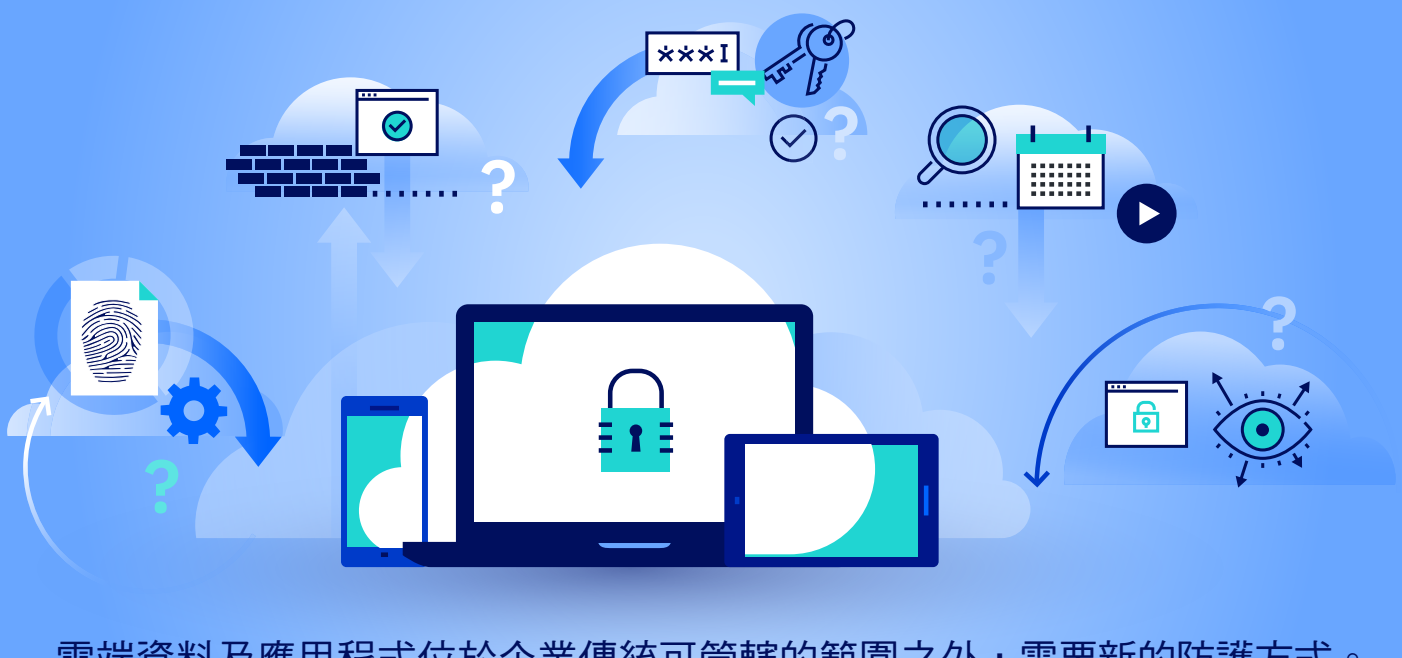
5 個基本雲端安全性問題



雲端資料及應用程式位於企業傳統可管轄的範圍之外，需要新的防護方式。確定您的提供者具備 您需要的所有能力。

身份識別與存取權限管理

1. 您的雲端平台 是否能整合我們公司的身份識別管理系統 - 或是提供值得信賴的替代方案？

雲端平台的交互作業就從驗證正在進行交互作業之人員或程式開始— 管理員、使用者，甚至是服務。尋找能一致提供服務的提供者：

- 識別及驗證可存取雲端平台的使用者
- 識別及驗證雲端上託管之應用程式的一般使用者
- 驗證 API 存取權限及服務呼叫的身份識別
- 將您現有的身份識別存取權限管理 (IAM) 系統與雲端平台整合

IBM Cloud™ 的開發人員可以使用 **App ID** 將自動驗證置入行動及 Web 應用程式。

安全的基礎架構

2. 您的雲端平台是否會依據工作負載而 提供 妥善整合的防火牆、值得信賴的運算主機及 微分割 的選項？

- **安全性群組及防火牆**— 網路防火牆對於保護周邊以及在執行個體層級存取權限建立網路安全性群組而言至為關鍵。
- **微分割**—將雲端原生的應用程式以一組小型服務的方式來開發可提供安全性優勢：您可以使用網路區段加以隔離。
- **值得信賴的運算主機**—硬體式主機安全性包含測量-驗證-啟動通訊協定，可提供絕佳防護以執行您的工作負載。

利用 **IBM Cloud Secure Virtualization** 並使用 **IBM Cloud** 信任的容器之容器應用程式，在值得信賴的平台上部署虛擬化工作負載。

資料加密與金鑰管理

3. 您的平台是否支援自攜金鑰？

自攜金鑰 (BYOK) 模式可讓您集中管理加密金鑰、確保根目錄金鑰絕對不會超出金鑰管理系統的邊界，而且可讓您稽核金鑰管理生命週期。

IBM Cloud 可利用 **IBM Cloud Key Protect** 服務為資料加密提供 BYOK 支援。

應用程式安全

4. 掃描容器化應用程式是否存有漏洞的頻率及範圍為何？

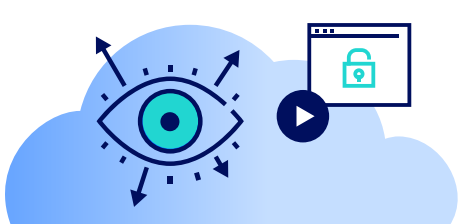
DevOps 團隊需要自動化安全性檢查。要求可持續掃描登錄鏡像及執行中容器之潛在漏洞的整合式工具。

IBM Cloud 容器服務提供 **Vulnerability Advisor**以提供靜態和即時容器影像掃描。

可見性及智慧

5. 您的安全性日誌檔及報告是否會反映多個可見點並與客戶 SIEM 整合？

內建雲端活動追蹤程式 可自動記錄及追蹤存取平台及服務的所有項目，包含 API、Web 及行動存取權限。您的組織應該可將那些日誌檔整合至安全性智慧及事件監控 (SIEM) 系統，讓您能夠 360 度檢視環境。



IBM® QRadar® 是全方位 SIEM 產品，可提供一組基於 AI 的安全性智慧解決方案，而可隨組織需求成長。

還有關於雲端安全性問題需要解答嗎？
請定期 **ibm.com**/cloud/security

39013839-TWZH-00