IBM **Cloud**

保護雲端平台的指南

目錄

IBM

關鍵要點

1 理想狀況下，雲端廠商應該要能夠將您公司的身份識別管理系統與他們的平台整合，並在任何情況下，都能視需要提供值得信賴的身份識別管理解決方案供您使用。

2 基於工作負載及值得信賴的運算主機，驗證雲端平台提供妥善整合的防火牆、安全性群組和微分割選項，這也是建立信任關係的一部分。

3 期望雲端廠商可提供 BYOK 解決方案，讓您的組織能專門管理所有資料儲存環境及服務之間的金鑰。

4 容器的最佳安全性實務是在部署之前和執行期間掃描容器是否存有弱點。

5 雲端平台安全性必須要有效地控制存取權限、在工作負載等級操作、詳細追蹤活動並整合至內部部署系統。

重新思考以雲端為基礎之應用程式的安全性

由於有越來越多組織改為使用雲端原生模式來開發應用程式和管理工作負載，雲端運算平台迅速限縮了 傳統以管理範圍為基礎之安全性模式的有效性 。當然, 本身的管理範圍安全性仍嫌不足。因為雲端中的資料及應用程式位於傳統企業管理範圍之外，所以必須以全新方式加以保護。

轉換至雲端原生模式或規劃混合雲應用程式部署的組織必須利用可保護以雲端為基礎之工作負載的技術，來補強傳統管理範圍為主的網路安全性。企業必須相信雲端服廠商能確保他們從基礎架構之上的堆疊安全無虞。選責廠商時，建立對平台安全性的信任感已經是重要基礎。

雲端安全性驅動因子

資料保護及法規合規性是推動雲端安全性的主要驅動力，它們也是阻礙企業採用雲端的因素。若要解決這些問題，通常要延伸至開發及維運的所有面向。雲端原生應用程式可能會在物件儲存、資料服務及雲端之間派送資料，造成多個潛在攻擊的端口。而攻擊不僅來自組織精密的網路黑幫和外部來源；根據最近的調查，53% 的受訪者確認在過去 12 個月期間也發生過內部攻擊。[1]

雲端安全性的五個基礎

由於組織需要解決使用雲端平台的專業安全性需求，他們需要且期望廠商能成為值得信賴的技術合作夥伴。事實上，組織應該根據安全性的這五個面向來評估雲端廠商，因為這些面向與組織自己的特定需求息息相關：

1. **身份識別與存取權限管理：**驗證、身份識別及存取權限控制
2. **網路安全性：**保護、隔離及分割
3. **資料保護：**資料加密與金鑰管理
4. **應用程式安全性及 DevSecOps：**包含安全性測試及容器安全性
5. **可見性及智慧：**為模式監控及分析日誌檔、流程及事件

驗證雲端平台上的身份識別和管理存取權限

雲端平台的交互作業就從驗證身份識別開始，取決於正在進行交互作業之人員或程式 - 管理員、使用者，甚至是服務。在 API 經濟中，服務就能採取自己擁有的身份識別，依據此身份識別而準確且安全地對服務進行 API 呼，這樣的能力對於成功執行雲端原生應用程式而言至為關鍵。

尋找能為 API 存取權限及服務呼叫一致地驗證身分識別的廠商。您也需要一個方法來識別和驗證可存取雲端託管之應用程式的一般使用者。例如，IBM® Cloud 會使用 App ID 作為開發人員將驗證與行動及 Web 應用程式整合的方法。

強勢驗證可防止未經授權的使用者存取雲端系統。因為平台身份識別及存取權限管理 (IAM) 是重要基礎，已擁有系統的組織應期望雲端廠商能與他們的身份識別管理系統整合。這通常會透過身份識別聯合技術支援，連結多個系統之間的個人 ID 及屬性。

為何需要驗證服務？

在以微服務為基礎的架構中，API 可讓應用程式彼此溝通和分享資料。應用程式執行時，使用 API 視需要呼叫服務，以完成各種作業。例如，您的應用程式可能會為資料呼叫物件儲存服務。物件儲存服務之後會呼叫金鑰管理服務取得加密資料所需的加密金鑰，這也是完成要求的一部分。而且在提供使用者體驗時，應用程式可能會使用 API 存取使用者身份識別資訊、在應用程式之間張貼內容 (例如，從應用程式章貼內容至 Twitter)，以及判定使用者伺服位置特定資訊的位置。**其中所有整合點都會面臨安全性挑戰。**

雲端廠商應該一致地驗證需要存取 API 或服務之使用者或服務的身份識別。當然，在驗證時，應該基於稽核目的記錄所有存取要求工作階段及交易。**API 及服務最有可能持有寶貴的智慧財產權，您不會希望有人使用這些服務。**

請雲端廠商證明他們的 IAM 架構及系統可涵蓋所有基礎。例如，在 IBM Cloud 中，身分識別及存取權限管理會以幾個重要功能為基礎 (圖 1)：

身份識別

- 每個使用者都有唯一的識別碼
- 會依據服務和應用程式的服務 ID 進行識別
- 會依雲端資源名稱 (CRN) 識別和處理資源
- 會對使用者及服務進行驗證並藉由其身份識別核發金鑰

存取權限管理

- 由於使用者及服務嘗試存取資源，IAM 系統會判定哪些存取權限及動作會遭到允許或拒絕
- 服務會定義動作、資源及角色
- 管理員會定義在各種資源上指派使用者角色及權限的原則
- 保護會延伸至 API、雲端功能及雲端託管的後端資源

您可以評估雲端廠商的安全性、尋找存取控制清單連同常見的資源名稱，因此不僅可將使用者限制在特定資源，還可限制為哪些資源上的特定作業。這些功能有助於確保您的資料可同時免於遭到未經授權的外部和內部存取，安全無虞。

當您使用 Enterprise IdP 的現有企業應用程式上建立雲端原生應用程式時，將您自己的企業身份識別提供者 (Enterprise IdP) 延伸至雲端特別有用。您的使用者可以順暢地同時登入雲端原生及底層應用程式，而不需要使用多個系統或 ID。降低複雜性永遠是值得努力的目標。

關鍵要點

理想狀況下，雲端廠商該要能夠將您公司的身份識別管理系統與他們的平台整合，並在任何情況下，都能視需要提供值得信賴的身份識別管理解決方案供您使用。

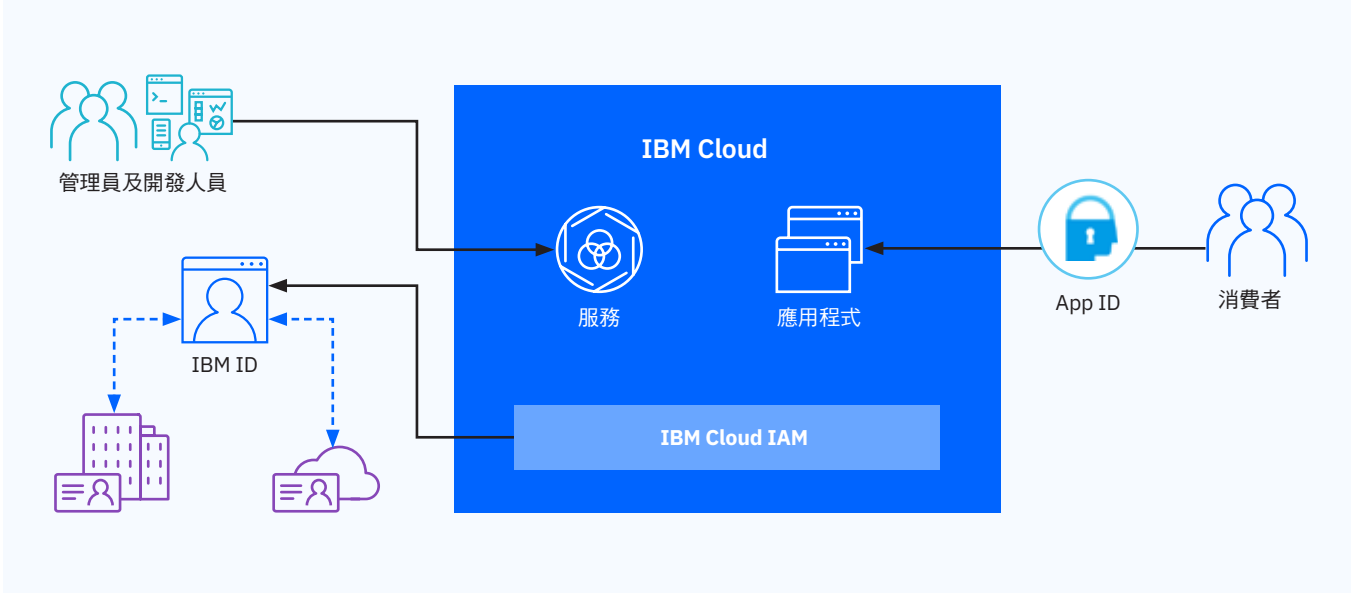

圖 1. 分隔廠商管理及客戶管理的叢集元素。

重新定義網路隔離及保護

許多雲端廠商會使用網路分割，限制對於同一個網路中的裝置及伺服器的存取權限。此外，廠商還能在實體基礎架構上建立虛擬隔離網路並自動將使用者或服務限制於特定隔離的網路。這些和其他基本網路安全性技術是在雲端平台中建立信任感的基礎。

雲端廠商提供保護技術 (從 Web 應用程式防火牆到虛擬私人網路和服務遭拒緩解)，以作為軟體定義網路安全性及使用費用之服務。在雲端運算時代中，將下列技術視為關鍵網路安全性。

安全性群組及防火牆

雲端客戶通常會插入網路防火牆以保護管理範圍 (虛擬私有雲/子網路等級網路存取權限) 並建立網路安全性群組以獲得執行個體等級的存取權限。安全性群組是將存取權限指派給雲端資源的第一道理想防線。您可以使用這些群組輕鬆地新增執行個體等級網路安全性，以便管理公共及私有網路上的入埠和出埠流量。

許多客戶都需要管理範圍控制能力來保護管理範圍網路及子網路，而且虛擬防火牆是可輕鬆符合此需求的部署方式。防火牆設計旨在防止不需要的流量流入伺服器，以及降低攻擊範圍。雲端廠商應提供虛擬及硬體防火牆，讓您針對整個網路或子網路設定以權限為基礎的規則。

當然，VPN 可提供從雲端返回內部部署資源的安全連線。如果您執行的是混合雲環境，這些就是必要項目。

微分割

以一組小型服務方式來開發雲端原生應用程式提供了安全性優勢，可使用網路分割予以隔離。尋找可透過自動化網路配置及網路佈建來部署微分割的雲端平台。**套用微服務模式的容器化應用程式已經快速成為支援擴充工作負載隔離的常態現象。**

關鍵要點

在工作負載及值得信賴的運算主機驗證雲端平台能提供妥善整合的防火牆、安全性群組和微分割選項，這也是建立信任關係的一部分。

利用資料加密與金鑰管理來保護資料

對於任何數位產業而言，可靠地保護資料是一項安全性基本工作 - 特別是在金融服務和醫療保健等高度規範的產業。

與雲端原生應用程式相關聯的資料可能遍及物件儲存區、資料服務及雲端。傳統應用程式可能有自己的資料庫、VM 和存在於檔案中的機密性資料。在這些情況下，同時加密靜止和移動中的機密資料就變得極為關鍵。

企業擔心雲端維運人員或其他未經授權之使用者未經其許可而存取資料，以及預期這類使用者可獲得完全可見性而存取資料，這都是很正常的現象。**利用加密來控制資料存取，同時也控制加密金鑰的存取，也變成期待的保護措施。**因此，自攜金鑰 (BYOK) 模式現在已經是一項雲端安全性要求。這可讓您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界線，而且可讓您稽核所有金鑰管理生命週期 (圖 2)。

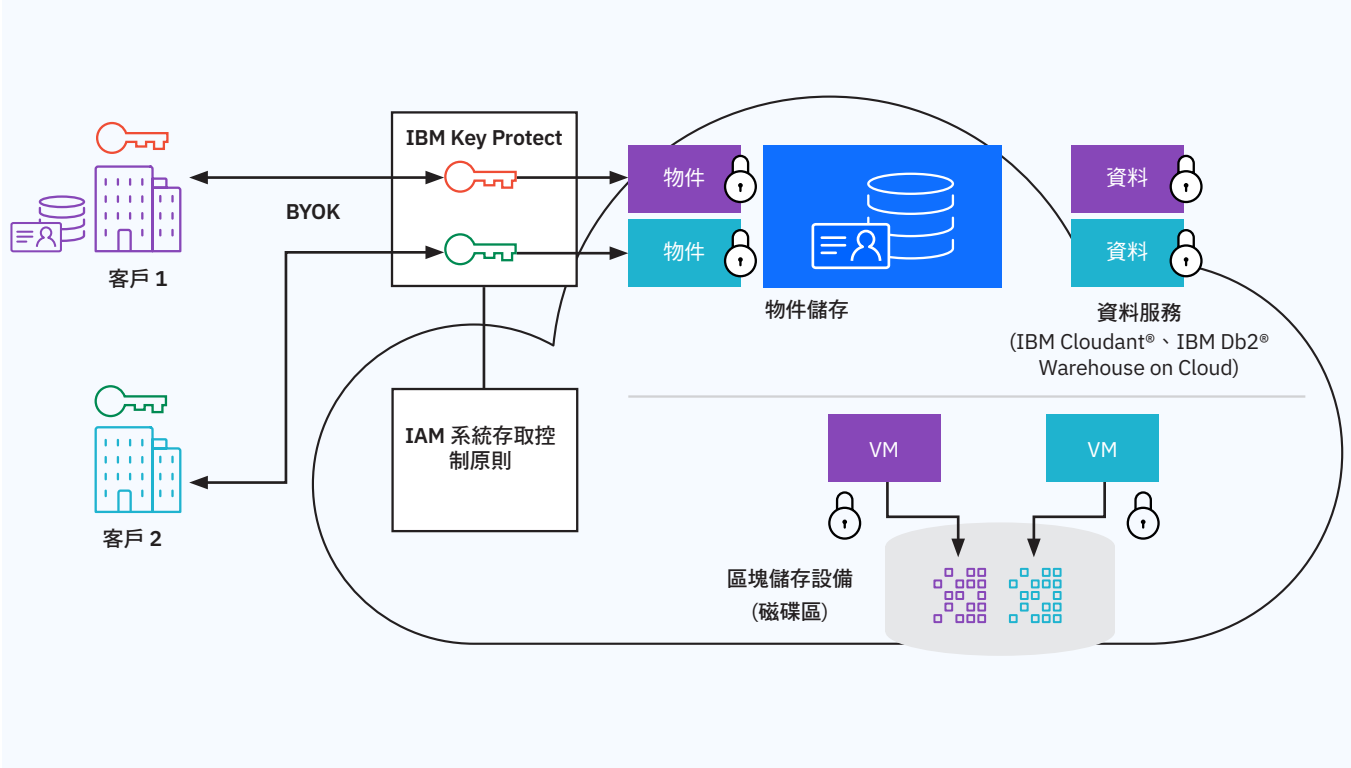

圖 2. BYOK 解決方案的架構。

值得信賴的運算主機

談到硬體：沒有人希望將寶貴的資料和應用程式部署在不受信賴的主機上。提供具有測量-驗證-啟動通訊協定的硬體雲端平台廠商，可為您提供高度安全的主機，將應用程式部署在容器調度系統中。

Intel Trusted Execution Technology (Intel TXT) 及 Trusted Platform Module (TPM) 是主機等級技術的範例，可為雲端平台建立信任關係。Intel TXT 會抵禦以軟體為基礎的攻擊，這類攻擊會透過毀損系統或 BIOS 程式碼來竊取機密資訊，或是修改平台的配置。Intel TPM 是以硬體為基礎的安全性裝置，會先確保系統啟動程序是防竄改設定，然後才將系統控制能力釋放到作業系統，藉此保護系統。

靜止和傳輸中的資料保護

BYOK 的內建加密可讓您維持對資料的控制能力，無論資料是位於內部部署或雲端中。這是控制他人存取雲端原生應用程式部署中資料的絕佳方式。藉由此方法，客戶的金鑰管理系統會在內部部署產生金鑰，然後傳送到廠商的金鑰管理服務。這個方法可在區塊、物件及資料服務等儲存類型之間包含靜止資料加密。

對於傳輸中的資料，安全通訊及傳輸會取代傳輸層安全性/安全通訊端層 (TLS/SSL)。TLS/SSL 加密也可讓您判定合規性、安全性及治理，而不需要取得密碼系統或基礎架構的管理控制能力。若要建立雲端平台的信任關係，需要具備管理 SSL 憑證的能力。

符合稽核及合規性需求

提供您自己的加密金鑰並將之保存在雲端 (不需要服務廠商存取權限)，可讓您看見和控制資訊安全長進行合規性稽核所需的資訊。

關鍵要點

雲端廠商應提供 BYOK 解決方案，讓您的組織能管理所有資料儲存及服務之間的金鑰。

為 DevOps 自動化安全性

隨著 DevOps 團隊建立雲端原生服務並使用容器技術，他們需要方法來整合日漸自動化的開發管道中的安全性檢查。Docker Hub 此類網站提倡公開交換資訊，開發人員只要下載自己需要的內容，就能輕鬆省下影像準備時間。但那樣的彈性代價是，開發人員必須例行性地檢查登錄中的所有容器鏡像，才能部署鏡像。

自動化掃描系統可協助確保信任關係，方法是先搜尋鏡像中的弱點，然後才開始執行鏡像。詢問平台廠商他們是否允許組織建立原則 (例如「不要部署有弱點的鏡像」，或是「將這些鏡像部署到正視環境之前先警告我」)，以作為 DevOps 管道安全性的一部分。

舉例來說，IBM Cloud Container Service 提供的 Vulnerability Advisor (VA) 系統，可同時進行靜態及即時的容器掃描。VA 會檢查雲端客戶私人登錄中每個鏡像的每個圖層，以偵測是否存有弱點或惡意程式，然後再部署影像。因為單純掃描登錄鏡像可能會錯過一些問題 (例如，從靜態鏡像到部署容器的漂移)，VA 也會掃描執行的容器是否有異常情形。也會以分層式警示提供建議。

關鍵要點

容器的最佳安全性實務是在部署之前和執行期間掃描容器是否存有弱點。

在 DevOps 開發通道中提升自動化安全性的其他 VA 功能包含：

- **原則違規設定：**藉由 VA，管理員就能依據三種類型的鏡像失敗情形來設定鏡像部署原則：包含已知弱點的已安裝套件；已啟用遠端登入；以及某些使用者可輕鬆猜到密碼並啟用的遠端登入。
- **最佳實務：**VA 目前會依據 ISO 27000 (包含密碼最短有效時間和密碼長度下限等設定) 來檢查 26 個規則。
- **安全性錯誤配置偵測：**VA 會針對每個錯誤配置問題設定旗標、提供描述並建議修復動作。
- **與 IBM X-Force® 整合：**VA 會從五個第三方來源抽取安全性情報，而且會使用已知修正程式的攻擊向數、複雜性及可用性對每個弱點進行評分。評分系統 (嚴重、高、普通或低) 可協助管理員快速瞭解弱點的嚴重性並排列補救動作的優先順序。

談到補救動作時，VA 並不會中斷執行中的鏡像而進行修復。相反地，IBM 會修復登錄中的「黃金」鏡像並將新影像部署到容器中。此方法可協助確保該鏡像的所有未來例證都會有相同的修正程式。VM 仍能以傳統方式處理，亦即使用端點安全性服務以修補 VM 並修正 Linux 安全性弱點。

談到 Kubernetes

如果您的 DevOps 團隊使用廣受歡迎的 Kubernetes 容器調度軟體，確保他們能持續使用偏好的工具。並評估平台如何輕鬆佈建新增和管理既有的 Kubernetes 叢集。

詢問雲端平台廠商是否可利用 Kubernetes 支援 Calico 及 Istio。Calico 及 Istio 是 Kubernetes 的兩個重要部分，可協助確保應用程式及工作負載安全性。Calico 有助於簡化在一個運算節點中指派 IP 位址給工作負載的管理作業，以及每個運算節點中的程式存取控制清單, 有助於增強安全性原則。使用原則定義設定並透過配置標籤強制執行，Istio 可針對 Kubernetes 容量或叢集的微服務之間，提供以憑證為基礎的控制能力。

透過智慧監控以建立安全免疫系統

移至雲端時，資訊安全長通常會擔心可見性偏低且喪失控制能力的問題。因為如果特定金鑰遭到刪除或配置不當地將變更伺服器返回內部部署資源或是企業安全性作業中心 (SOC)的連線，組織的整個雲端都可能會當機，維運工程師為何不應該要求雲端工作負載、API、微服務 - 所有內容 - 的完整可見性呢？

存取軌跡及稽核日誌檔

所有使用者及管理存取權限 (無論是由雲端廠商或您的組織提供) 都應該自動登入。內建雲端活動追蹤程式可以建立存取所有平台及服務 (包含 API、Web 及行動存取) 的軌跡。您的組織應該要能夠使用這些日誌檔並將之整合到企業 SOC 中。

企業安全性情報

確定您已經選擇將所有日誌檔及事件整合至內部部署安全性資訊和事件管理 (SIEM) 系統 (圖 3)。某些雲端服務廠商也提供包含事件管理及報告功能的安全性監控、安全性警示的即時分析，以及混合部署之間的整合式檢視。舉例來說，IBM QRadar® 是全方位的 SIEM 解決方案，可提供一組能隨組織需求擴充的安全性情報解決方案。其針對威脅模式提供的機器學習功能訓練，可建構預測安全性免疫系統。

代管的安全性及專業知識

如果您的組織沒有大量安全性專業知識，請尋找可為您管理安全性的廠商。某些廠商可以監控您的安全性事件、應用來自各個產業的威脅情報，以及與此資訊相互關聯以採取行動。詢問他們是否也能提供單一虛擬管理平台，以整合內部和代管安全性服務。

關鍵要點

雲端平台安全性必須要有效地控制存取權限、在工作負載等級維運、詳細追蹤活動並整合至內部部署系統。

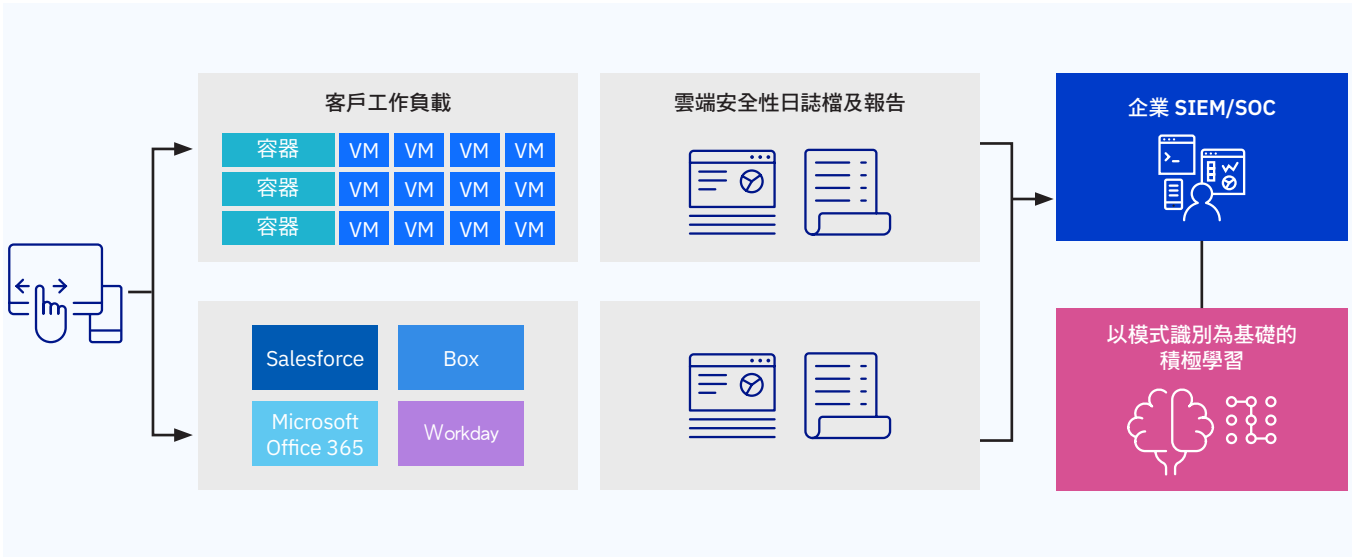

圖 3. 將雲端可見性整合到企業 SIEM/SOC.

促進企業成功的安全性

由於雲端技術對於執行數位業務而言，規模越來越大且更趨重要，通常需要尋找能夠提供一組適當的功能及控制能力的雲端廠商，以便保護面對客戶之應用程式所仰賴的資料、應用程式及雲端基礎架構。平台安全性解決方案應涵蓋五個主要雲端安全性重點區域：身份識別及存取權限；網路安全性；資料保護；應用程式安全性；以及可見性及智慧。目標是減少對於技術的憂慮並專注於您的核心業務。

受到妥善保護的雲端可提供重大的業務及 IT 優勢，包含：

- **縮短實現價值的時間：**由於已經安裝和配置安全性，團隊就能輕鬆佈建資源和迅速建立使用者體驗的原型、評估結果並視需要重複執行。
- **降低資本支出：**在雲端中使用安全性服務可盡量減少許多前期成本，包含伺服器、軟體授權及設備。
- **減輕管理負擔：** 藉由成功在雲端平台中建立和維持信任關係，具有適當安全性產品的廠商會承擔管理的最大責任，從而降低報告及資源維護的成本。

如需更多資訊

若要深入瞭解雲端安全性的五個重要領域以及 IBM 提供的相關技術及服務，請造訪：ibm.com/cloud/security

保持聯繫，掌握動態

IBM Cloud 部落格

關注我們

@IBMcloud
Facebook

與我們交流

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

美國印製 2018 年 1 月

[1] 內賊威脅 2018 年報告 - 於 2017 年 11 月發佈，
http://crowdresearchpartners.com/portfolio/insider-threat-report