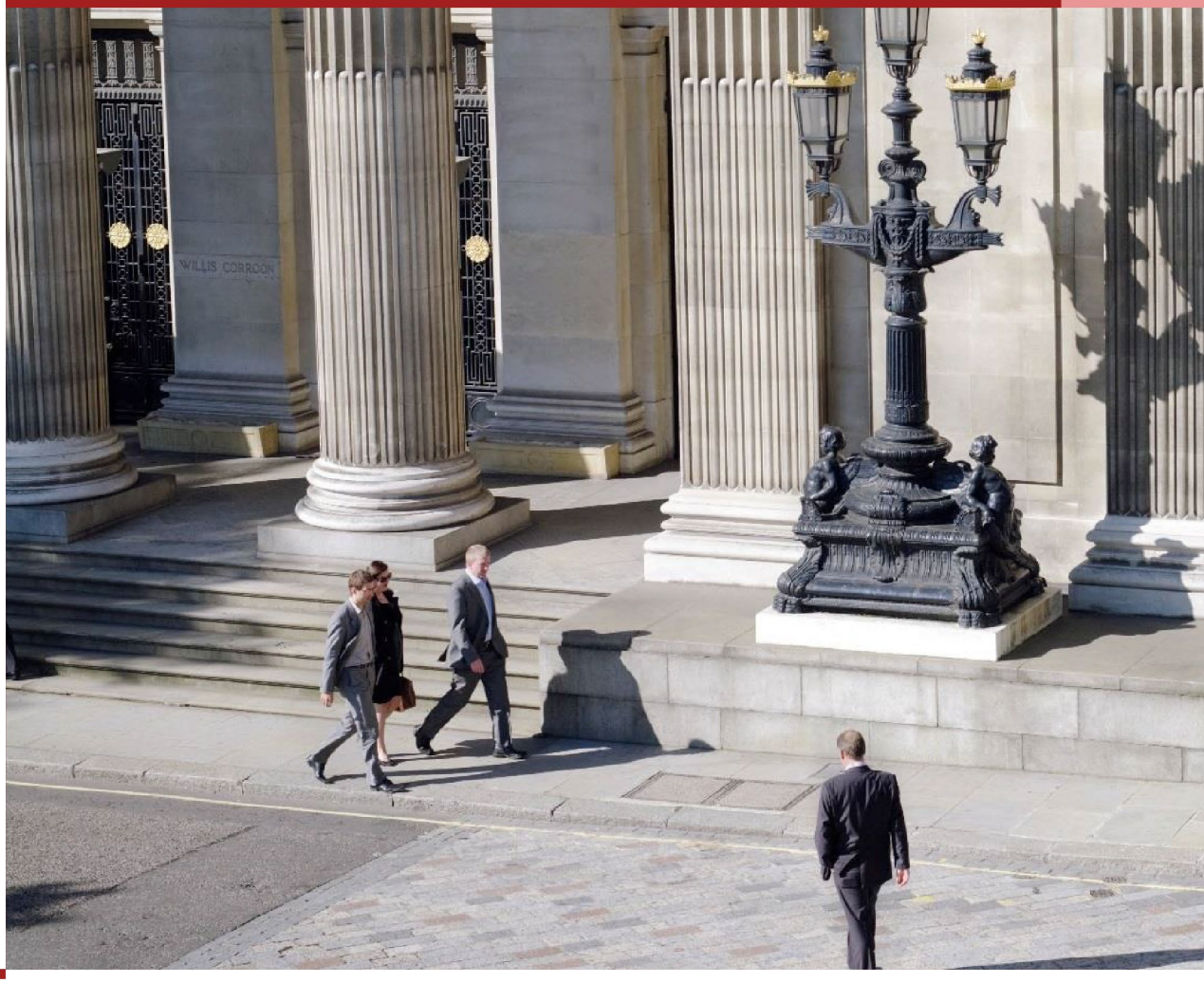
www.pwc.com/cybersecurityandprivacy

建置安全的 DevOps 流程

CYBERARK

2017 年 12 月



pwc

目錄

透過 DevOps 加速創新步伐

在當今的數位化世界裡，許多 IT 部門正努力適應快速發展進步的業務環境。所有企業，不管來自哪個業界 都正大力提高數位化程度，以便更好地與員工、合作夥伴及客戶合作。數位化管道正繼續從根本上改變業務模式 推動營收成長。

在當今快速發展的數位化時代，傳統的應用程式開發與管理方法通常顯得效率與靈活度不足。高瞻遠矚的企業正將目光投向 DevOps（將軟體發展、整合、測試與維運實踐融爲一體），以加速數位化轉型並改進業務績效。

DevOps 是一系列理念、方法與工具的綜合體，可以協助企業更快速且具成本效益地交付應用程式與服務。DevOps 利用敏捷且精簡的軟體發展原則與實踐來加強工程、品質保證與運營團隊間的協作並提高工作效率。

透過消除自成體系的職能與管理孤島，並自動完成變更管理、組態設定管理與部署流程，DevOps 可有助於開發部門快速上市時間，提高產品品質並降低成本。

連續開發、整合與交付方法使工程師可以快速且高效率在產品設計流程中納入使用者回饋，有助於提高企業靈活性，並且更快速回應客戶需求。

敏捷的企業可更快速增加營收 37%，增加利潤 30%

資料來源：《企業如何在動盪時期生存下來並發展壯大》。經濟學人智庫。

DevOps 帶來新的資安挑戰

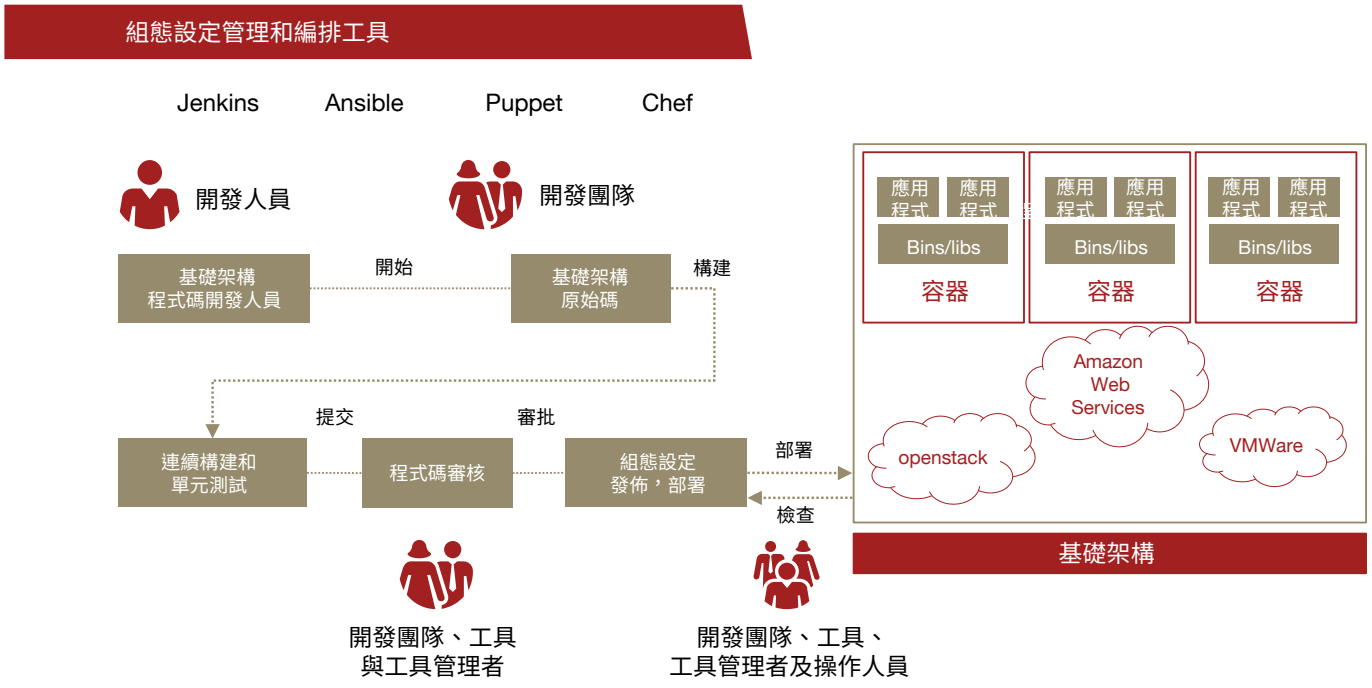
DevOps 使 IT 資安團隊面臨各種挑戰。DevOps 流程包括各種開發、整合、測試與部署工具、人員及資源，包括：

- 自動化組態設定管理平台與服務協作流程解決方案，旨在簡化開發並實現 IT 自動化。
- 公司內與雲端中的運算及儲存資源，用於建置、測試、維護與執行程式碼。
- 一組專業技術人士，包括開發人員、品質保證(QA)工程師與系統管理者，各有不同的角色與特權。

DevOps 生態系統的龐大規模與多樣性使企業很難保護：

- 每種開發與測試工具、組態設定管理平台與服務協作流程解決方案，各有自己的資安憑證或帳密；這些憑證或帳密一般透過不同的系統獨立進行維護與管理。
- secrets 資訊（密碼、SSH 金鑰、API 金鑰等），用於資料交換前的身份驗證並加密交易，廣泛散落在不同機器與應用程式中，因此幾乎無法追蹤與管理。
- 雪上加霜的是，開發人員通常透過寫死的 secrets 資訊嵌入到可執行程式檔中，使企業面對惡意攻擊與保密資料洩露不堪一擊。

DevOps 鏈中涉及的各種工具、人員與資源 *



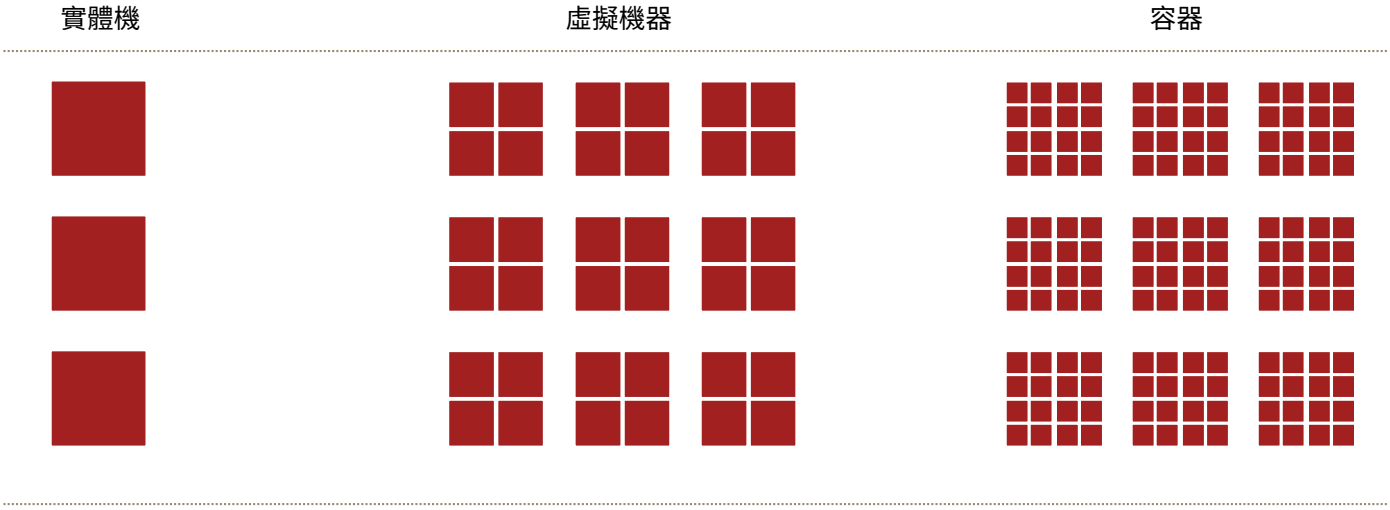
* 本圖重點顯示 DevOps 例子，並未顯示所有內容

容器加劇資安挑戰

許多 IT 部門利用容器化解決方案來增加營利，簡化連續開發與交付流程。容器包含完整的執行環境——應用程式、應用程式所依賴的所有單元以及設定檔，所有這一切都被組合到一個輕量產品套件中。利用容器，操作人員團隊就可以輕鬆地將應用程式從開發環境遷移到測試階段再遷移到線上環境中，而不需要調整軟體相關設定或更新執行環境。

容器可以消除傳統伺服器虛擬化解決方案的開銷與低效性。（使用伺服器虛擬化解決方案時，每台虛擬機器（VM））都執行自己的記憶體密集型虛擬作業系統。而利用容器化解決方案時 所有容器都使用同一作業系統）。虛擬機器可能有數千兆之規模，而容器大小可能只有數十兆。因此，實體伺服器可以託管比虛擬機器更多的容器。

容器導致 Secrets 資訊蔓延——每個容器都有獨特的資安屬性



容器的快速成長使 IT 部門面臨的資安挑戰更加嚴峻。在任何一家企業中，數百台虛擬機器可能輕鬆讓位於數千或數十萬個容器——各有自己獨特的資安屬性。更加糟糕的是，容器通常是短暫的（增加或拆除以支援連續交付），因此很難進行追蹤與管理。

DevOps 要求更可擴展而且敏捷的資安方法

傳統資安方法用於支援傳統企業應用程式與服務，不是非常適合動態多變的 DevOps 環境與雲端運算。許多資安團隊在整個交付鏈中依賴多種不同的身份驗證與授權解決方案。

自成體系的資安系統與實踐無法滿足連續開發與交付團隊提出的更高延展性與敏捷性需求。若 DevOps 流程的每個步驟都獨立進行保護，使用不同的工具，將影響到了服務速度。每種應用程式與機器都會引發安全性漏洞，增加受創面，使攻擊者有機可趁。而資安團隊缺乏對整個交付鏈從頭到尾地控制與可視性，因此增加了風險與不確定性。

利用脫節、自成體系的資安方法，管理者不能輕鬆完成以下工作：

- 在整個流程內制定通用身份驗證和授權計畫以實作統一安全性原則。
- 撤銷 secrets 資訊或鎖定系統以應對資安威脅或攻擊。
- 產生整個交付鏈的組態設定記錄並存取日誌，評估安全性漏洞或支援合規性審核。

DevOps 要求採用一種全新的方法來完成 secrets 資訊管理與存取控制——一種可以統一報告與管理、消除人爲延遲、增強程式設計功能與自動化的集中方法。

加速 DevOps 速度的工具 – CyberArk Conjur Enterprise

DevOps 速度的 secrets 資訊管理

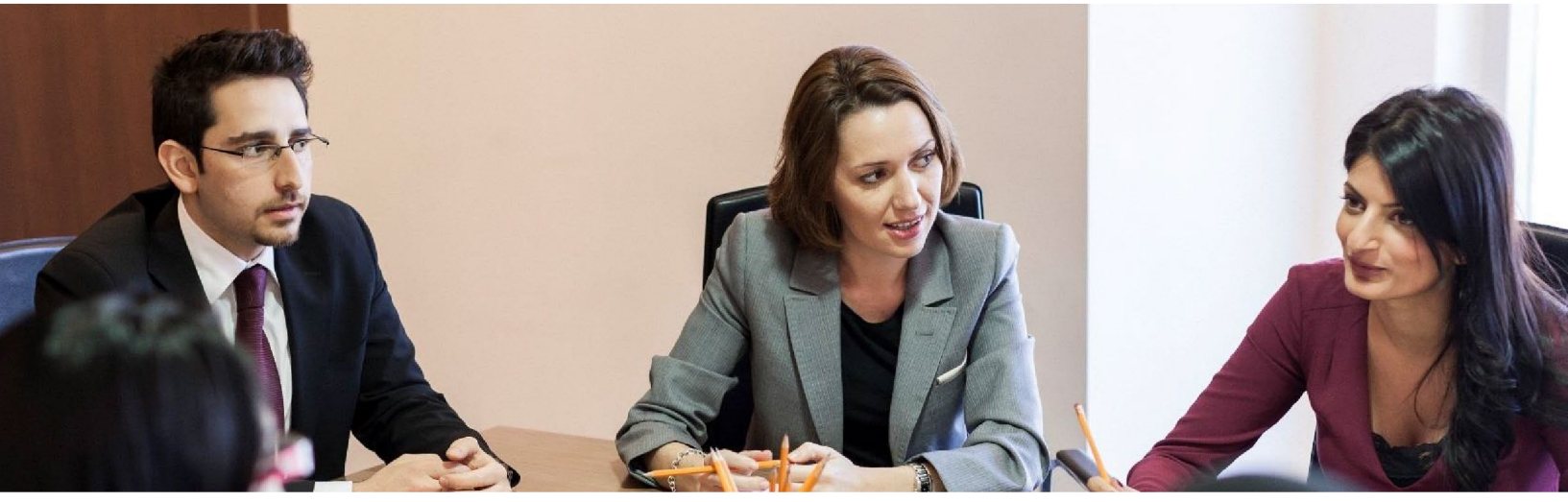
CyberArk 的 Conjur Enterprise 是一款市場領先的 secrets 資訊管理解決方案，設計用於滿足當前 DevOps 與雲端運算環境提出的更高延展性與敏捷性要求。此款解決方案旨在協助資安部門高效率保護與管理整個 DevOps 流程內機器、應用程式及使用者所使用的 secrets 資訊。在這方面，PwC 與客戶密切合作，利用部署與設定 CyberArk Conjur Enterprise 解決方案的豐富經驗來協助客戶管理 DevOps 流程內使用的 secrets 資訊。

此款解決方案可以集中管理整個 DevOps 流程（包括程式碼、伺服器、虛擬機器、服務、容器等）內的機器身份與基於角色的存取控制，協助 IT 部門簡化操作，同時在整個流程內

制定統一的安全性原則。Conjur 還可以協助企業增強安全性，緩解風險並達到嚴格的合規性要求而不降低工作流程速度。此款解決方案安全地保存 secrets 資訊、金鑰、憑證與身份驗證資料（儲存庫外原始程式碼外、硬碟機外），因此可實現有效的保護、控制與管理。

這種獨立於平台的 secrets 資訊管理解決方案專門設計用於容器化環境——在這種環境中，每個容器都分配到一組獨特的基於角色的存取特權，以實現精細的控制。容器中執行的應用程式與服務都以獨特的方式進行身份驗證與授權，確保 secrets 資訊可以安全地共用，而且只能與想要的目標接收方共用。

此外，此工具可以無縫地整合各種組態設定管理平台與服務協作流程解決方案，而且可以大規模部署在公司內或各種雲端環境中。此工具還可以整合現有的 Active Directory、LDAP 與 SIEM 系統，有助於企業保護並繼續利用原來的投資，沿用原有的資安模式與實踐。



Conjur 基於可提供高可用性與性能的分散式彈性架構。解決方案元件可以分佈在不同分區、地區與雲端中，以大幅縮短延遲，確保高延展性並消除單點故障。該解決方案利用 AWS Auto Scaling Groups 等功能來實現無限彈性的擴展，以支援大規模負載，而不降低系統性能。Conjur 解決方案的其它功能特性包括：

Secrets 資訊管理

有效地管理機敏性資料，如 API 金鑰、憑證、密碼、SSH 金鑰及權杖。secrets 資訊被安全保存在經過加密並受到存取控制的容器中，在這裡受到有效管理，而且可以根據原則自動定期更新。

基於角色的存取控制

權責分工，不同的使用者群組或機器輕鬆被分派不同的特權。管理者可以定義各種角色（如開發、測試、維運與管理），而且可以爲每種角色分派存取特定資源（如資料庫密碼、虛擬機器或伺服器、Web 服務終端等）的單獨全縣（如讀、寫與刪除）。

集中保存、防篡改的稽核記錄

收集及查看授權事件及 secrets 資訊操作，並產生合規性報告。

DevOps 工具鏈整合

保護並管理連續開發與整合工具（如 Ansible、Chef、Jenkins 與 Puppet）及容器協作流程軟體（如 Docker 與 Kubernetes）使用的 secrets 資訊。

整合現有資安系統及實踐

整合 Conjur 到其它安全解決方案與元件中，包括 CyberArk 特權帳號安全解決方案、Active Directory/LDAP 實作及協力廠商的 SIEM 解決方案。

簡便易用的 GUI

透過直觀的圖形使用者介面監控使用者、機器與 secrets 資訊；查看稽核記錄；組態設定原則與基於原則的工作流程。

企業優勢及功能總結

優勢	功能
提高 IT 速度	整合上游開發與維運任務中的資安與控制功能，加快服務速度，同時在所有線上系統中確保一致性
減少安全性漏洞並降低風險	透過整合並集中 secrets 資訊管理來最大幅度減小受創面
保護資產與保密資料	對所有容器、應用程式與使用者實作統一存取控制與權限分派
實作資安原則	確保遵守企業原則與政府監管要求

攜手 PwC，透過 DevOps 加速 IT

DevOps 不是一種工具或產品，而是一種維運方法。透過統一開發、品質保證（QA）與運營流程，實現基礎架構部署流程自動化與標準化，企業可以加速創新與上市時間，提高部署品質與運營效率，將更多精力集中於實現核心業務目標。

為什麼

透過逐步改進來降低交易成本以增加業務優勢。

什麼

透明度、一致性與協作，瞭解每個產品版本導致的 IT 與客戶環境的變化。

如何

繼續發展演進的方法與工具。

誰

開發人員、品質保證（QA）與維運人員。

PwC 基於 DevOps 理念開發的 High Velocity IT 解決方案擴展核心 DevOps 理念，協助完成各種任務與活動，來將理念轉變爲有用的以技術爲中心的實用功能。PwC 提供連貫的功能來協助客戶快速設計、建置並交付強大而且安全的系統。此款解決方案可以協助開發與維運團隊利用 CyberArk Conjur 打造高度資安而且敏捷的 DevOps 流程。

High Velocity IT 可實現以下目標：

- 更快速將理念轉變爲基於技術的功能
- 更低的交付成本
- 應用程式錯誤的早期偵測
- 更少的線上系統錯誤
- 更高的開發流程安全性
- 符合企業原則與政府監管要求
- 基於具體指標的持續改進
- 更高的人員與技術資源利用率
- 能夠在整個交付過程中預見並解決問題

結語

全球各地的企業都將目光轉向 DevOps，希望用 DevOps 來推動創新並加速數位轉型。自成體系的傳統資安系統與實踐不能滿足當今連續開發與交付環境提出的嚴格敏捷性與延展性要求。

PwC 擁有雄厚的實力，與客戶密切合作來識別、設計並部署適用於 DevOps 的更先進流程與技術解決方案，如 CyberArk Conjur。我們與 CyberArk 合作的豐富經驗使 IT 部門可以高效率管理 DevOps 流程內的存取與授權特權，協助資安團隊降低風險並改進合規性而不影響工作流程。

PwC 與 CyberArk 有著廣泛的業務合作關係，而且在設計與實作 CyberArk 解決方案方面擁有非常豐富的經驗。CyberArk 在 2016 年與 2017 年將 PwC 評爲美洲區年度最佳全球系統整合商。

PwC 與 CyberArk 可以協助企業建置資安而敏捷的 DevOps 流程來實現高速 IT。

連絡人

若欲瞭解更多資訊，請聯繫：

Chris Hall
主管，**PwC**
g.christopher.hall@pwc.com

Rich Kneeley
董事總經理，**PwC**
richard.j.kneeley@pwc.com

Mickey Roach
合夥人，**PwC**
mickey.roach@pwc.com

Matt Lawson
主管，**PwC**
matthew.d.lawson@pwc.com

Alex Coassin
主管，**PwC**
alexander.t.coassin@pwc.com

Rohit Antao
主管，**PwC**
rohit.antao@pwc.com

Sowvik Chakrabarty
總監，**PwC**
sowvik.chakrabarty@pwc.com

Scott Whitehouse
副總裁，**CyberArk**
scott.whitehouse@cyberark.com

www.pwc.com/cybersecurityandprivacy