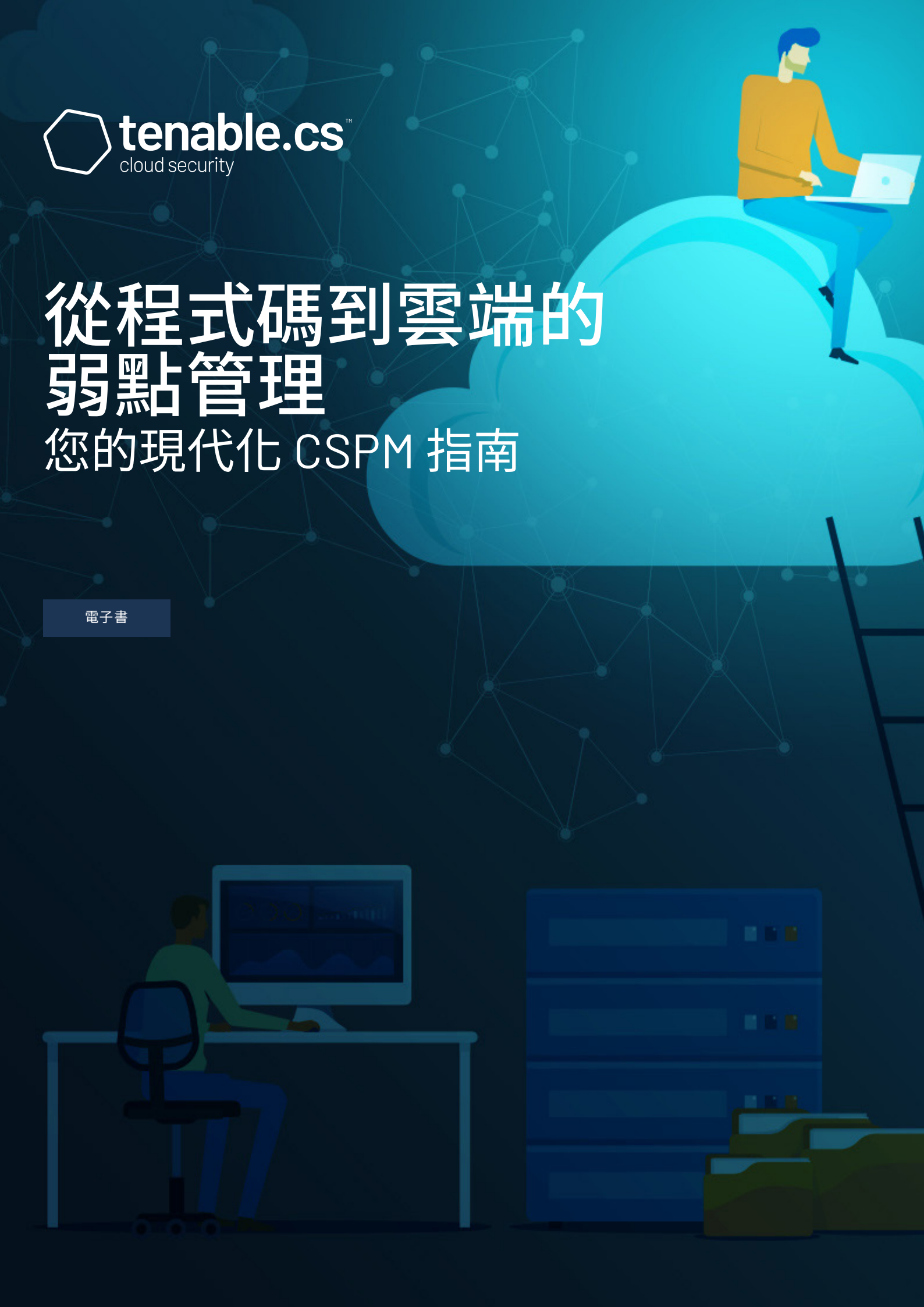
tenable.cs™
cloud security

從程式碼到雲端的弱點管理

您的現代化 CSPM 指南

電子書



目錄

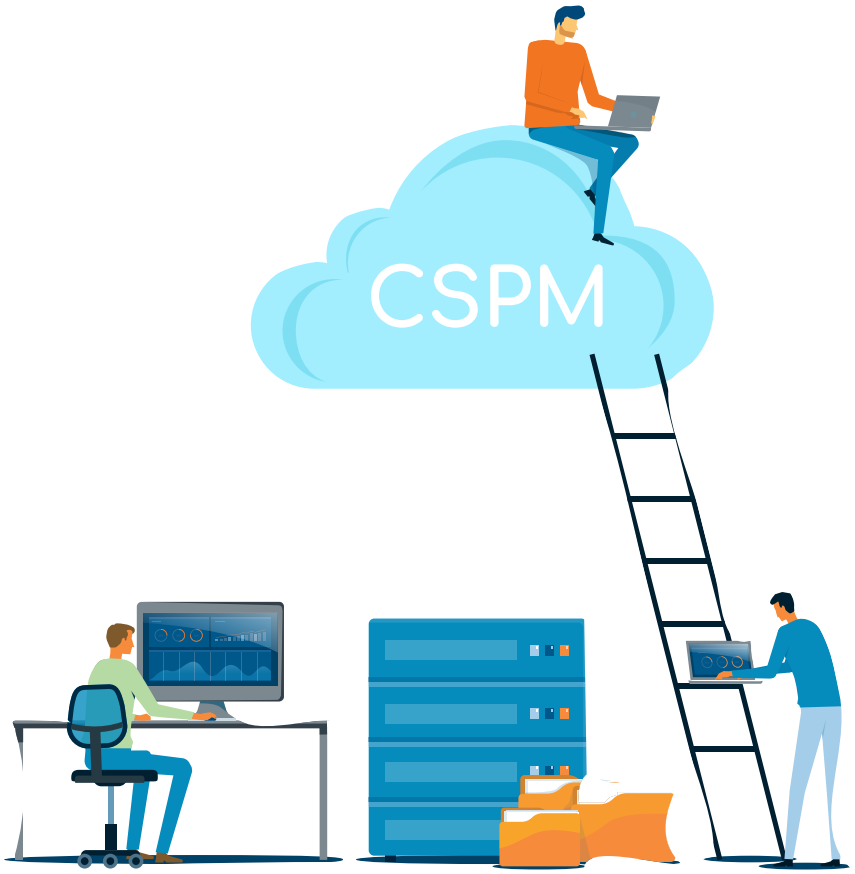
將弱點管理拓展至雲端，保護執行階段與開發的安全

身為現代的資安長、資安主管或企業安全團隊的任何一份子，每當思及「我們有多安全？」這個大哉問，肯定讓您徹夜難眠。

迅速吸納今日的技術才能造就未來創新，但這麼做也造成企業的基礎架構愈發複雜，同時帶來全新的挑戰。不論是採用內部部署、雲端或混合式架構，企業在其整體環境中的風險無所不在。如今不單只有資料中心算是關鍵資產，這就表示任何一個基礎架構面向都會成為攻擊破綻的關鍵要害。這也是為何將弱點管理拓展至整個攻擊破綻會是解答「我們安全嗎？」這個大哉問的良方。如同您搜尋、排序和解決傳統 IT 資產中的軟體弱點，公司現在必須確保對雲端基礎架構採取同樣的動作。它們需要取得其所有雲端資源和資產的完整能見度並持續不斷地進行曝險修復，且最好所有操作都能集中在單一平台中。主要需提防的弱點有三個：軟體缺陷、身分資料外洩和設定錯誤。公司需盡全力偵測並修復這幾種弱點，了解弱點所屬的資產類型及其確切位置。

安全團隊必須能夠辨認出最高風險的結果，與開發和營運團隊進行有效溝通，幫助他們了解結果的意涵及修復方式，進而形成所謂的「DevSecOps」結構。對負責保護企業和客戶資產安全的安全團隊來說，他們需要一個雲端安全態勢 (CSPM) 解決方案，能夠幫助他們建立並強制執行從程式碼到雲端的安全和合規性原則。

公司需仰賴傳統的執行階段安全工具來獲取其雲端環境弱點的能見度，以及解決既有部署資源的現存風險。然而，公司也需要在整個軟體開發週期和供應鏈中偵測並修復軟體缺陷、身分資料外洩和設定錯誤。至少公司應設想確保開發流程安全的必然性。這包含加速交付修復的程式碼，確保迅速修復風險並降低安全團隊的負擔，且開發人員用不著成為安全專家就能做到。這就是企業的 DevSecOps 發展之路的基石。這也是為何採用雲端安全態勢 (CSPM) 解決方案以及採取精進策略，將安全工作提早納入的公司，能夠在不妨礙營運速度的情況下進行建置工作，同時將整體風險降至最低。



雲端安全態勢管理：走向主流

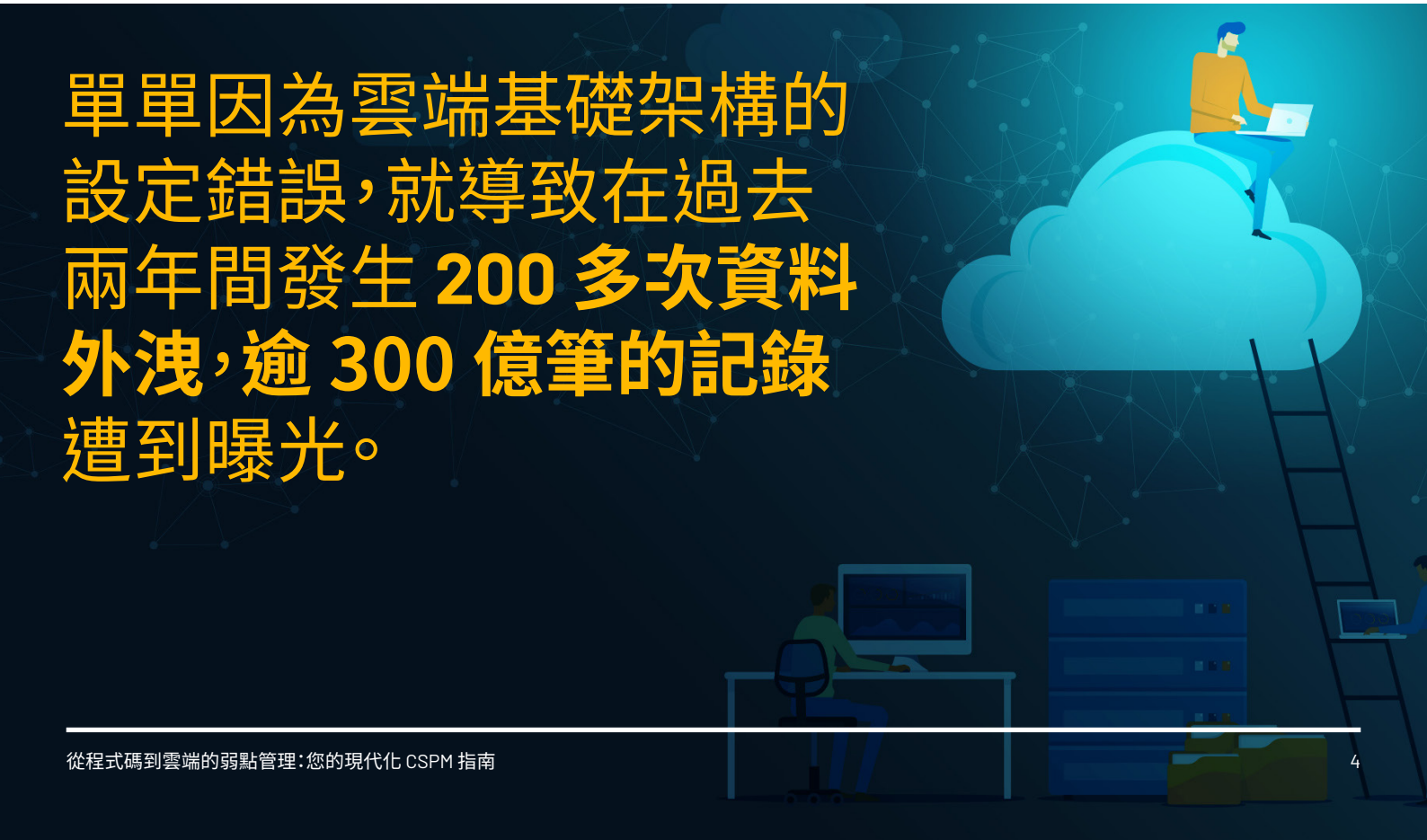
要是說人們的所有生活層面因為 COVID-19 而遭逢嚴重停擺，這種說法是過於輕描淡寫了。最明顯的影響是雲端基礎架構的轉變，它讓原本需要兩年時間才能完成的數位轉型，在某些情況中壓縮到只在兩個月內便已達成。這種發展走向促使大環境需因應並支援大幅提升的遠距辦公數位化與彈性需求，同時還得提供客戶全新的服務和機制，以維繫客戶與公司之間的生意往來。

企業加快採用雲端基礎架構的腳步，而雲端服務供應商也對此做出回應。但是，雲端資安外洩的規模和速度也不斷加劇。**單單因為雲端基礎架構的設定錯誤，就導致在過去兩年間發生 200 多次資料外洩，逾 300 億筆的記錄遭到曝光。**

企業飛快地採用雲端服務和基礎架構，使得出錯的空間持續加大，這意味著強化網路的穩定性已刻不容緩。為了解決雲端設定錯誤的問題，CSPM 解決方案自 2013 年開始興起，但時至今日 CSPM 已自成一格，且更被普遍認定為雲端安全管控機制的主流。根據分析師的說法，這項技術之所以屬於「現在進行式」的範疇，原因在於企業大量採用許多相近的安全技術，並可開始觀察到其蔚為主流的端倪。尤其對於必須遵守 HIPAA、HITECH、DFAR 等其他合規要求的企業而言更是如此。

現在就開始設法運用 CSPM 的企業，勢必會在此關鍵技術獲得廣泛採用的未來中取得領先地位。本指南主要是在闡述評估 CSPM 解決方案時需納入考量的關鍵要素。

單單因為雲端基礎架構的設定錯誤，就導致在過去兩年間發生 200 多次資料外洩，逾 300 億筆的記錄遭到曝光。



傳統 CSPM

建立執行階段的安全設定基準，以及監控是否有偏離基準的情況，是 CSPM 背後的普遍原則。企業可以運用 CSPM，透過下列基本流程找出一般的安全設定錯誤：

1. CSPM 解決方案透過 API 連接到執行階段雲端環境，評估有風險的設定。
2. 緩解風險之後，CSPM 解決方案會建立執行階段的基準。
3. 新的基準定義完成後，後續若出現偏離此基準的變更，CSPM 同樣會在執行階段中偵測出來並進行風險評估。
4. 某些 CSPM 解決方案有提供自動修復功能，可將設定還原成執行階段的安全基準。

對於在執行階段中定義和管理的雲端原生架構而言，此方法原本應是可行的解決方案。然而，這個假設不再成立。近期的 CNCF 調查發現在當今的雲端基礎架構中，有很大一部分在開發期間是以程式碼進行定義和管理。熱門的基礎架構即程式碼 (IaC) 技術包括：

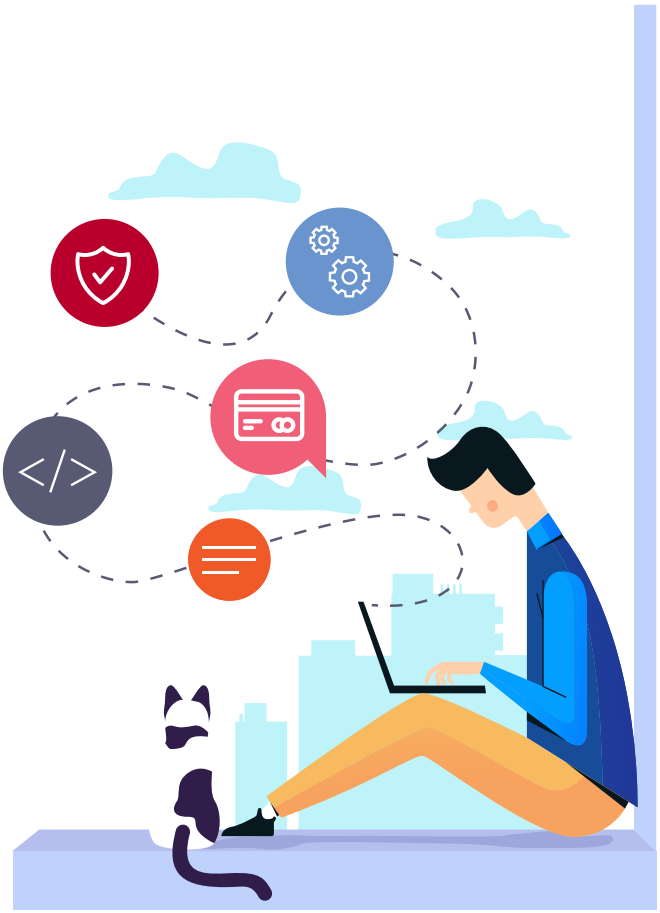
容器：
有高達 92% 的企業在正式作業環境中使用

Kubernetes：
有高達 83% 的企業在正式作業環境中使用

無伺服器：
有高達 30% 的企業在正式作業環境中使用

專家預期這樣的趨勢會持續上升，也意味著開發時會招致設定錯誤，造成佈建出存有風險的雲端架構。因此，基準必須在更早的週期階段建立完成，CSPM 才能真正發揮效用。

執行階段 CSPM 解決方案的固有缺陷為：它們雖然能夠偵測出這些設定錯誤，但在執行階段解決風險的代價過於高昂。結果就只能放任絕大部分的問題不管，不但為攻擊者製造了進攻時機，更遑論會對企業產生的多大的責任。最重要的是，變更執行階段中的設定來解決風險會引發另一個問題：該設定變更不會反映在 IaC 中，亦即倘若採用 IaC 重新部署雲端架構，修復的設定也將消失無蹤。最好的情況是白白浪費了時間、金錢和資源；最糟糕的情況則是讓組織產生安全的假象。



改採新世代 CSPM 的理由

依賴雲端並轉成使用基礎架構即程式碼技術的企業急遽增加，現有的 CSPM 解決方案顯然得有所精進才不至於落後。如今我們需要全新的 CSPM 方法，它要能夠在開發期間偵測並解決設定錯誤，同時維繫執行階段的安全態勢。只要遵守三個重要宗旨就能做到這一點：

1. 保護基礎架構即程式碼的安全

第一步是要在編寫程式碼的開發期間啟動流程。這表示必須在開發期間掃描 IaC，偵測並解決設定錯誤，建立安全基準。如此方可確保佈建出無風險、「天生安全」的雲端基礎架構。

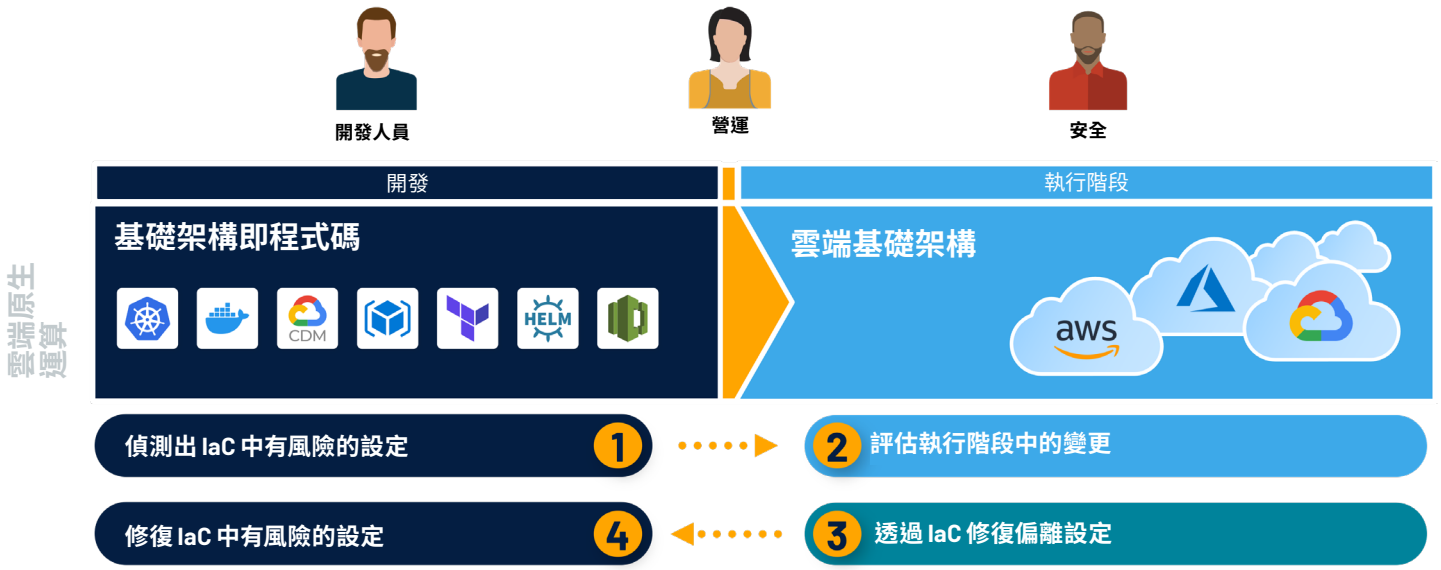
2. 監控執行階段中的基礎架構設定

我們一定要假設使用者會在執行階段中變更設定，因而逐漸造成偏離設定的情況。因此，持續監控是維繫安全環境不可或缺的一環。使用安全的 IaC 基準完成基礎架構佈建之後，持續監控執行階段中的設定並偵測變更。

3. 透過基礎架構即程式碼進行修復

偵測到的任何變更都必須進行風險評估。新世代 CSPM 的不同之處在於，它一律是以 IaC 作為單一事實來源的參考依據。只要一出現會構成風險的變更，即會依據安全的 IaC 基準重新部署雲端。如果變更不至於構成風險，則會更新 IaC 以反映該變更並據此建立新的 IaC 基準。這麼一來即可確保執行階段中的正確設定變更不會消失。

此概要說明可幫助您為將來的雲端安全發展鋪路，讓您得以透過新一代 CSPM 解決方案獲得實質效益。本指南後面幾個小節將深入剖悉實現各宗旨所必須具備的重要功能，並列出購買 CSPM 之前應考量的問題。



宗旨 #1：保護基礎架構即程式碼的安全

一定要在開發流程中及早偵測基礎架構即程式碼中的設定錯誤(IaC)，並為開發人員提供即時的意見回饋，因為這有助於提高解決風險的可能性。因此，當開發人員在其儲存庫中提交程式碼的同時，也必須持續掃描 IaC，但是要及早且低調的進行。只要採用具備熱門的整合式開發環境(IDE)或原始碼管理(SCM)工具的 CSPM 解決方案，就能達成上述目的。以下要點說明新世代 CSPM 解決方案會採行哪些步驟，確保在您的 IaC 中建立安全基準。

IaC 支援的幅度

保護 IaC 安全的困難之處在於 IaC 的衍生者眾多，但不同類型的 IaC 卻欠缺標準化的基礎架構定義。舉例來說，Kubernetes YAML 與 Terraform 的 HashiCorp Configuration Language(HCL)截然不同。欠缺標準化造成難以用統一的原則集和威脅模型來評估和緩解風險。唯一可達成一致性的可擴充方法，便是將不同類型的 IaC 標準化為統一格式(雲端即程式碼)。評估 CSPM 解決方案時，探討 IaC 支援的幅度是非常重要的，如此才能確保支援貴組織目前使用的關鍵技術。

合規性與監管

定義標準化基礎架構之後，可統一套用基於原則的查核(原則即程式碼)，找出違反合規性或安全最佳做法的漏洞。常見的違規例子包括：

- **開放公眾存取的雲端儲存服務**
- **網際網路上的公開 SSH 連接埠**
- **開放的安全群組**

CSPM 發揮成效的關鍵在於，程式碼必須在其開發期間進行審核，但又不會妨礙開發人員的工作流程和靈活性。Tenable.cs 提供 1,800 個立即可用的原則，開發人員可在其工作流程中運用並整合這些原則，亦可選擇建立自訂原則。評估 CSPM 解決方案時，您應該期望它具備完善可靠的原則庫，以及便於建立自訂原則的特性。還有一點值得注意，Open Policy Agent(OPA)已成為強制執行原則的新標準。舉例來說，相較於利用 Rego 查詢語言的 OPA 型原則，Python 型原則引擎的使用靈活度就差了一截。

預測資料外洩路徑

在基礎架構即程式碼不停變動的高速開發環境中，原則即程式碼會產生大量警示，進而導致人員對警示感到疲乏。事實上，最近有一項研究發現對警示感到疲乏而引發的震驚結果：只有 4% 偵測到的問題可以真正獲得解決。從現實面來看，並非所有風險都同等重要，因此必須有方法可以評估各風險的曝險和可利用性，以安排解決問題的優先順序。例如，同樣是存在弱點的容器，它在私有子網路中的風險一定低於暴露在網際網路上的風險。Tenable.cs 利用威脅模型化技術來評估並排定威脅的優先順序，這代表您可以知道必須優先關注哪些警示。它藉由分析基礎架構即程式碼，了解所要定義的資源項目、資源設定方式及兩者間的關係來建立威脅模型。這有助於我們判定設定錯誤是否會構成架構中的潛在外洩路徑。無論是哪一個 CSPM 解決方案，都應該要考量到它能否透過威脅模型化來偵測風險(安全即程式碼)，以強化其本身的原則即程式碼功能。

程式化修復

程式化風險偵測一定要搭配程式化修復功能，才能確保安全防護跟得上開發的速度。但是，絕大多數的開發人員都不是安全專家，對於如何修復在 IaC 中偵測到的設定錯誤一無所知。修復工作流程必須能夠與開發人員的工作流程整合，還要能協助開發人員解決風險問題。唯一可擴充的方法便是採用會自動產生解決設定錯誤所需的程式碼，並對主要分支提出提取要求 (修復即程式碼) 的 CSPM 解決方案。此方法不但可以維持開發人員的開發速度，還能確保程式碼的品質。

CI/CD 整合的幅度

提交程式碼之後，多數企業會利用 CI/CD 工作流程持續建置和部署基礎架構。這是確認佈建的雲端基礎架構不會帶有設定錯誤的最後機會。最重要的是 CSPM 解決方案必須整合 CI/CD 工具，才能持續提供安全防護，避免部署設定錯誤的基礎架構。選擇 CSPM 工具時，務必探查 CI/CD 整合的幅度，確認它可以支援貴組織使用的核心工具。

購買 CSPM 的重要必問問題：

- **支援哪些類型的 IaC？**
- **提供多少預先定義的原則？**
- **支援哪些合規性和安全標準？**
- **使用何種查詢語言來定義自訂原則？**
- **解決方案如何在開發期間找出潛在的資料外洩路徑，以及安排解決問題的優先順序？**
- **解決方案可以自動產生解決設定錯誤的程式碼，建立提取問題以協助開發人員嗎？**
- **解決方案整合了哪些 CI/CD 工具，可避免佈建設定錯誤的基礎架構？**

宗旨 #2：監控執行階段中的基礎架構設定

解決基礎架構即程式碼中的設定錯誤之後，接下來會建立安全基準並部署基礎架構。理論上應該要禁止在執行階段中對基礎架構做任何設定變更，所有變更都必須透過 IaC 進行，基礎架構才能保持不變。然而，實際情況卻大相逕庭。基於各種理由，雲端基礎架構的設定變更確實會在執行階段中發生，這種情況可以說是家常便飯。Tenable 在最近的一項研究中發現，有超過 90% 的企業允許使用者在執行階段對雲端基礎架構進行設定變更。如此一來，依據 IaC 安全基準持續監控執行階段的基礎架構變更就變得格外重要。

執行階段環境的程式碼化

為了比較執行階段中的基礎架構變更與 IaC 基準的定義，必須將執行階段中的基礎架構變更轉換為程式碼（雲端即程式碼）。如此能為在執行階段中建立的資源與透過 IaC 定義的資源提供確定性的比較方式。同樣地，它也可以為執行階段中的資源設定與 IaC 中的資源定義提供確定性的比較方式。實質上來說，執行階段設定必須經過反向工程以進行程式碼化，這就是新一代與前兩代 CSPM 之間最大且最根本的架構差異。

偏離 IaC 基準

由於 IaC 並非支援所有的執行階段資源，因此難免會在部署完基礎架構之後進行部分資源的定義和更新。因此，CSPM 解決方案必須有能力偵測現有資源是否有出現不同於 IaC 基準定義的設定變更（偏離即程式碼），亦即設定偏離的情況。它也要能偵測出偏離 IaC 基準的新建資源與終止資源，亦即資源偏離的情況。常見的偏離情況包括安全群組設定與 IAM 原則的變更。

合規性與監管

察覺並管理偏離是鞏固基本安全防護的關鍵。一旦找出偏離之後，必須立刻進行評估以判定其是否有違反合規性與最佳安全做法。確保統一化監管並利用跟評估 IaC 時所使用的相同原則集（原則即程式碼）是非常重要的。

預測資料外洩路徑

偏離同樣必須經過評估來判定其是否會構成潛在的資料外洩路徑。我們可以透過建立威脅模型達到此目的。如果變更確實會構成潛在的資料外洩路徑，那麼比起嚴重性較低的風險，應該優先修復此問題。

購買 CSPM 的重要必問問題：

- **支援哪些執行階段環境？**
- **解決方案能否相對於透過 IaC 定義的安全基準，找出建立或終止的資源？**
- **解決方案能否找出不同於 IaC 基準定義的資源設定變更？**
- **解決方案能否在執行階段中套用評估 IaC 所使用的相同原則集？**
- **解決方案如何在執行階段中找出潛在的資料外洩路徑，並安排解決問題的優先順序？**

宗旨 #3：透過基礎架構即程式碼進行修復

第一代與新一代 CSPM 解決方案之間存在的最大差異，就是它們如何修復在執行階段中構成的偏離情況。第一代 CSPM 解決方案的修復功能會自動變更執行階段中的設定變更，這種方式只能解決一小部分的風險。這種方式反而會讓風險倍增：

- **它必須允許 CSPM 工具更新執行階段環境，對於具有高度安全意識的企業來說，這可能有違其公司政策的規定。**
- **允許工具自動對執行階段基礎架構進行設定變更會構成潛在的停機風險。**
- **最重要的是，變更執行階段中的基礎架構設定會造成偏離 IaC 基準。這也意味著倘若使用 IaC 重新部署基礎架構，在執行階段中所做的變更也會消失無蹤。**

相較之下，新世代 CSPM 解決方案會建立 IaC 作為單一事實來源。以下是兩種不同情境下的風險處理方式：

無風險的變更範例：為了增進應用程式的效能，工程師提高了執行階段中某個運算執行個體的記憶體設定。執行階段中的這個設定變更並不會構成風險，因此會更新相應的 IaC 以反映該變更，同時建立新的 IaC 基準 。只要使用修復即程式碼即可做到這一點，它會自動產生更新 IaC 的程式碼，並透過提取或合併要求將程式碼傳送給適當的開發人員審核。

有風險的變更範例：工程師不慎在路由表中建立一個規則，導致包含敏感資料儲存庫的子網路暴露在網際網路上。如果執行階段中的設定變更會構成風險 ，則會根據 IaC 基準的安全設定產生解決問題的程式碼 (修復即程式碼)。接著營運團隊即可使用程式碼重新部署基礎架構，消除變更所造成的風險。

購買 CSPM 的重要必問問題：

- **出現執行階段變更時，解決方案會自動產生解決問題的程式碼嗎？**
- **解決方案能否以程式化方式建立提取或合併程式碼的要求，藉此更新 IaC 並修復執行階段中產生的偏離？**

總結

現代生活在各方面幾乎都會牽涉到雲端運算，從醫療保健及交通，乃至農業和商業活動都與之息息相關。**個人和企業每天仰賴逾 350 億個雲端連線裝置，與親友交流、進行商業交易、提供防衛與關鍵基礎設施支援等。到了 2025 年，雲端裝置的數目將倍增為 750 億台。**

這些雲端應用程式和服務的安全、防護力和可用性，以及它們的網路穩定性至關重要，但是資料外洩的規模和範圍也不斷加大。**光是在過去三年來，就有逾 300 億筆記錄在雲端中曝光**。攻擊手法變得更加複雜精妙，且越來越常鎖定供應鏈作為目標，假冒受信任的廠商散布惡意軟體，企圖操控終端使用者系統、惡意利用關鍵資料庫或勒索企業牟利。

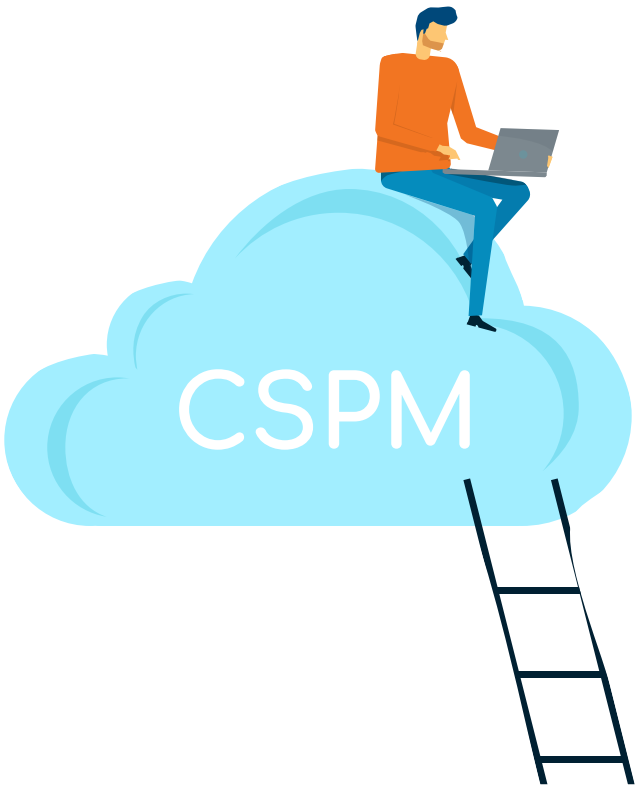
擁有統一的資源能見度，且有能力偵測和修復整個雲端執行階段環境中的弱點，對於保護雲端基礎架構安全是一個不錯的起點。不過，套用修復的時機點過晚，使得在執行階段中找出的風險早已曝光在攻擊者面前，且下次部署時套用在執行階段中的修復會完全被覆蓋掉，這些都是支持提早執行安全性的 CSPM 有力的論點。

傳統的安全防護軟體模式不足以偵測和避免資料外洩，因為軟體的開發和交付隨著移至雲端環境而出現本質上的不同。開發人員在軟體驅動經濟中的掌舵地位更甚以往。他們編寫的程式碼不單只有支援應用程式，更要支援基礎架構和自動化流程的運作，且這樣的情況越來越常見。只要提交一個不良的程式碼，就可能為攻擊者創造可供其惡意利用的資料外洩路徑。

評估現代化 CSPM 解決方案時，一定要尋找可透過 IaC 技術，藉由程式化方式偵測和解決開發期間的設定錯誤，並可維繫執行階段安全態勢的解決方案。這個方法可實現網路穩定架構與安全性，確保迅速的 DevOps 協作。達到此目標的必要功能：

1. 原則即程式碼
2. 安全即程式碼
3. 修復即程式碼
4. 偏離即程式碼

實現這些功能的唯一方法便是將數種不同類型的 IaC 及執行階段雲端環境的設定加以標準化，實質上就是將您的雲端程式碼化。下面的檢查清單是一份詳盡的問題列表，可協助您進行提早執行安全工作的 CSPM 相關評估。



現代化 CSPM 檢查清單

保護基礎架構即程式碼的安全

- ❑ 支援哪些類型的 IaC？
- ❑ 提供多少預先定義的原則？
- ❑ 支援哪些合規性和安全標準？
- ❑ 使用何種查詢語言來定義自訂原則？
- ❑ 解決方案如何在開發期間找出潛在的資料外洩路徑，並安排解決問題的優先順序？
- ❑ 解決方案可以自動產生解決設定錯誤的程式碼，建立提取問題以協助開發人員嗎？
- ❑ 解決方案整合了哪些 CI/CD 工具，可避免佈建設定錯誤的基礎架構？

監控執行階段中的基礎架構設定

- ❑ 支援哪些執行階段環境？
- ❑ 解決方案能否相對於透過 IaC 定義的安全基準，找出建立或終止的資源？
- ❑ 解決方案能否找出不同於 IaC 基準定義的資源設定變更？
- ❑ 解決方案能否在執行階段中套用評估 IaC 所使用的相同原則集？
- ❑ 解決方案如何在執行階段中找出潛在的資料外洩路徑，並安排解決問題的優先順序？

透過基礎架構即程式碼進行修復

- ❑ 出現執行階段變更時，解決方案會自動產生解決問題的程式碼嗎？
- ❑ 解決方案能否以程式化方式建立提取或合併程式碼的要求，藉此更新 IaC 並修復執行階段中產生的偏離？

關於 Tenable

我們 Tenable 認為提早執行弱點修復的方式可以讓企業放心發揮雲端的創新能力。我們提供端對端的整合式資安解決方案，使企業在保護他們的雲端環境時更得心應手。此解決方案可以透過深入程式碼、設定、資產與工作負載的統一能見度，提供整個新型攻擊破綻的網路風險全貌。深入瞭解 Tenable.cs，探索我們的平台如何實現以 IaC 為重心，透過整合開發和執行階段工作流程管控，實現 DevSecOps 模式。

tenable®