FIREEYE™

產品型錄

雲端運算架構和資安評估

透過更好的雲端架構和設定改善網路防禦

主要優點

- **瞭解**您的特定雲端環境架構面臨的威脅
- **減少**常用雲端架構的錯誤設定
- **減少**常用攻擊技術的攻擊面
- **瞭解**與現有設定有關的主要資安風險
- **增強**雲端監控、可見性和偵測
- **針對雲端環境進行適當的安全性強化的優先順序**

為何選擇 FireEye Mandiant

FireEye Mandiant 自 2004 年以來就站在網路資安與網路威脅情報的最前線。我們的資安事件回應團隊站在全球最複雜入侵事件的最前線。我們對現有和新興的威脅發動者以及他們快速變動的戰略、技術與程序，皆有深入的瞭解。

概觀

為了降低成本和提高擴充性，組織紛紛將內部資產遷移到雲端。因此，攻擊者開始重新調整其策略和技術，包括社交工程和利用錯誤設定，瞄準雲端環境。

FireEye Mandiant 雲端運算架構和資安評估可評估您目前的資安狀態，並為最常用雲端平台上的資產提供需要強化的優先順序建議：Microsoft Azure、Amazon Web Services 和 Google Cloud Platform。

此項評估可幫助貴組織瞭解特定雲端環境特有的威脅和資安控制，強化環境以抵禦目標威脅，並提高您在整個攻擊生命週期中的所有階段偵測、調查和回應攻擊者活動的能力。

這些服務是為使用支援基礎架構即服務 (Infrastructure as a Service, IaaS) 或平台即服務 (Platform as a Service, PaaS) 模型的雲端服務提供者的組織設計的。這些模型依靠雲端服務提供者和客戶共同抵禦網路事件。我們的評估側重於強化資安態勢的客戶責任。

我們的作法

評估分為四個階段，在這些階段中，Mandiant 專家將繪製現有雲端環境，並確定您目前的資安計畫如何保護環境：

第 1 週：初始文件檢閱，與客戶利益相關者在異地對遷移策略、體系結構圖、強化文件、存取管理策略和標準、SOP/手冊和日誌記錄標準進行檢閱。

第 2 週：現場工作坊，探討您的雲端環境、現有的資安模型以及未來要實施的潛在資安概念和控制，以配合您的業務需求。

第 3-4 週：從雲端平台進行設定檢閱，以確保有效實施資安控制，發現潛在漏洞並從現場工作坊總結經驗教訓，從而識別可被攻擊者利用的潛在漏洞。

第 5 週：詳細列出實用技術建議的報告，強化雲端環境、增強可見性和偵測能力，並改進流程以降低漏洞風險。

產出成果

Mandiant 提供的評估後報告包括

- 目前雲端環境快照，詳細介紹了現有架構和資安控制。
- 特定雲端服務的安全性與您目前的設定和操作流程保持一致。
- 增強可見性和偵測能力的實用建議。
- 進一步強化雲端架構的優先順序和詳細的建議。

按要求提供技術級和執行級簡報。

在評定期間，評估的核心重點領域。

管理、風險與合規性	資安架構和網路	身分和存取管理
• 雲端管理和服務	• 雲端架構和資安控制	• 雲端認證基礎架構，包括內部連接（如 ADFS）
• 雲端策略和標準	• 網路分段和內部整合	• 身分管理
• 威脅風險評估	• 遠端系統連接和管理	• 權限存取管理
• 漏洞管理	• 災害復原	• 角色為主的存取控制
• 監管合規要求	• 容器、設定和資安控制	
機密和資料保護	**開發運維**	**威脅偵測與回應**
• 資料保護和遺失預防	• 管道設定	• 系統、資料庫和應用程式日誌記錄
• 資料庫安全性	• 系統和應用程式部署	• 資安記錄和集中化
• 證書和金鑰管理	• 資安軟體發展生命週期	• 端點和網路資安控制
• 加密	• 代碼庫資安控制	• 雲端事件回應流程

要知道更多關於 FireEye，請前往：**www.FireEye.com**

FireEye Taiwan | 台灣火眼有限公司
10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE
taiwan@FireEye.com

關於 FireEye, Inc.

FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸，提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平台。藉由此方法，FireEye 得以讓對於準備、預防及回應網路攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。

M-EXT-DS-US-EN-000236-01