CLOUDVISORY：
多雲端環境可視性、合規性及管理

對於許多組織而言，管理複雜的多雲端環境並不是一種選擇，而是無可避免的處境。對雲端安全性的投入不斷地在增加，但其並沒有跟上雲端平台使用量的增加。

FireEye Cloudvisory 透過雲端原生整合與控制提供完整的雲端安全解決方案，以實現持續的可視性、合規性及管理，從而簡化資安工作。Cloudvisory 對目前雲端安全趨勢所揭露的問題做出補救。

35%*的組織認為雲端供應商應負責保護敏感或機密資訊

雲端供應商確實有很多內建安全效能，但那些並不夠堅固。客戶組織要負責在雲端保護他們自己的資料。Cloudvisory 揭示了雲端供應商未透露的重要發現，匯集來自多個雲端環境的資料，並強調資訊安全團隊需要採取行動的資料。

70%*的安全團隊表示，在雲端環境中管理隱私與資料保護條例，要比在其組織內部管理網路複雜得多

Cloudvisory 是雲端原生、多雲端管理的唯一全面解決方案，它執行以 CIS、GDPR、HIPAA、NIST、PCI 和 OpenStack Security Checklist 為基礎的最佳實踐方式，讓集中化的團隊更容易清晰地確定其責任。

56%*的組織表示，使用雲端資源會增加合規風險

Cloudvisory 為多帳戶、多雲端及多作業系統環境提供持續的合規保證，能自動透過可設定的檢查來偵測已知資產、控制及事件中的風險。Cloudvisory 合規提供超過 1,300 個內建的可自訂合規檢查，而且還能增加更多檢查項目。

只有 50%* 的組織定義了保護敏感雲端資訊之責任，儘管事實上，有 48%*的所有企業資料是儲存在雲端中

Cloudvisory 使用各種模型來自動分析所有網路設定，並推薦改進設定的具體活動。團隊可以使用 Cloudvisory 安全遙測（security telemetry）來將變更的測試自動化，直到他們確信這些變化能真正減少其風險。

一般的企業會使用 29*款雲端應用程式，這會導致資安複雜性提高

Cloudvisory 為雲端及 OS 供應商提供廣大的支援，包括 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP)。Cloudvisory 能夠快速安裝並與現有資安工具整合，以便所有團隊能清楚地看到其多雲端環境中的活動。

55%*的美國組織相信他們擁有雲端計算應用程式、平台或基礎設施服務使用的可視性

Cloudvisory 儀表板提供所有已連接的基礎設施之安全的全面可視性。持續資產發現是完全自動化的，而且 Cloudvisory 能即時維護每個服務提供者的多個帳戶中的所有範圍內資產的全面清單，將每個工作負載映射到已發現的風險。

FIREEYE CLOUDVISORY

對大多數企業而言，管理複雜的多雲端環境是個現實問題。將這些環境整合到用於監控和管理的集中式解決方案中，有助於更好地控制他們目前正在面對的管理、合規性及可視性問題。

FireEye Cloudvisory 是雲端安全管理的控制中心，能為任何雲端環境提供可視性、合規性及管理。資產發現和合規性掃描等雲端原生微服務，可實現複雜多雲端環境的威脅偵測與回應的端到端自動化。

Cloudvisory 是唯一一個不僅能為您
所有的多雲端、多作業系統環境提供最佳保障的安全解決方案，同時也提供對保障未來投資的回報，且推動持續的效率與資安性改進。

若要瞭解更多有關 Cloudvisory 的內容，請參閱：www.FireEye.com/cloudvisory

*Ponemon Institute（2019 年）。保護雲端資料（Protecting Data in The Cloud）。2019 年 Thales 雲端資安研究。全球版。