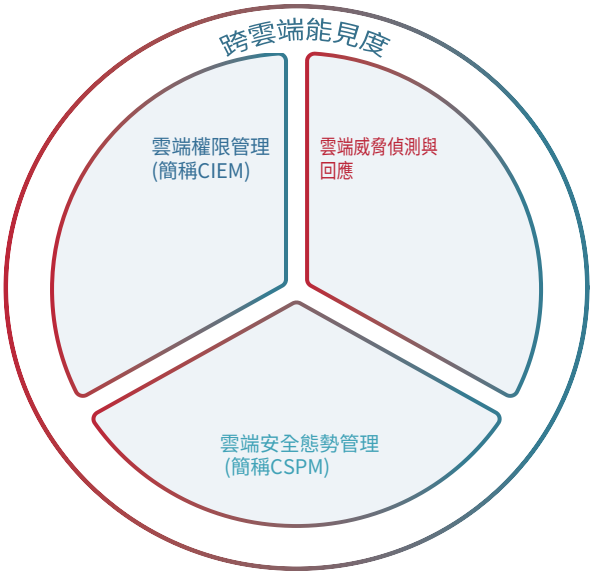
針對公用雲的全方位防護

頻繁地在雲端管理工作負載意味著會逐漸失去對雲端資產的控制與能見度。雲端環境是以遠端方式管理且會更換頻繁，因而讓資安團隊難以檢測與追蹤資產、監督對敏感資源的存取，或管理橫跨多個公有雲的安全性。因此，很多組織無法成功偵測及防止雲端基礎架構的攻擊。

Radware 提供一種免代理、易於部署的雲端原生解決方案，能適用應用程式、工作負載，以及在 Amazon 網路服務 (簡稱 AWS) 及 Microsoft Azure 上託管的基礎架構。Radware 的雲端原生保護方案提供多層級的防護機制以降低資安風險包括透過持續對照多個安全標準以驗證合規性、辨識已公開曝露的資產、持續追蹤資產庫存與優先排序的跨雲端能見度、透過智能強化機制強化雲端威脅破口，並且提供進階攻擊偵測與阻止資料竊取的補救能力。



跨雲的能見度與控制

Radware 使用單一管理控制平台及支援包含 AWS 與 Azure 的多雲環境，提供集中的工作負載安全管理。另外也能自動發現雲端資產庫存，以及統一檢視在單一主控台內橫跨多個雲端帳戶、區域與環境的資產。

從雜訊中抽離出有用的資訊

告警通知

使用許多不同的惡意行為指標（Malicious Behavior Indicator，簡稱 MBI）辨識可疑活動。

關聯分析

運用關聯分析機制檢視攻擊狙殺鏈，建立統一的攻擊序列

整治修復

使用風險基礎觀點與警示，在威脅發展成駭侵之前加以封鎖

先進的威脅偵測與風險優先排序

一鍵式合規報表

提供多種合規標準的立即可用報告格式，實現全方位的合規報告。

顯示量化風險

使用內建警示評分有效率地排列優先順序，可統一檢視多個雲端環境與帳戶。

持續偵測配置錯誤的問題

偵測配置錯誤與公開曝露的資產，以強化雲端態勢及減少攻擊威脅破口。

智能強化建議

提供優先的風險建議，完整說明風險內容與建議補救的措施。

進階偵測惡意行為

使用 70 多個MBI 辨識可疑行為，例如異常的儲存讀取、網路活動或資料外洩。

智能顯示攻擊的關聯性

顯示個別可疑事件的關聯性並整併成攻擊軌跡，搭配攻擊狙殺鏈的顯示攻擊步驟。