面向公有雲的全面保護措施

混雜的許可權是託管在公有雲上的計算工作負載面臨的頭號威脅。在公有雲環境中，很容易就可以授予過多許可權，但對這些許可權進行追蹤就非常困難了。因此，雲工作負載很容易受到資料洩露、帳戶入侵和資源利用等的侵擾。Radware提供了一個無代理的雲端原生解決方案，可以全面保護AWS和Microsoft Azure資產，並保護雲環境的整體安全態勢以及針對雲端原生攻擊向量的單個雲工作負載。雲端原生防護服務可以檢測工作負載的混雜許可權，在資料洩露發生之前強化安全配置，並利用先進的機器學習演算法檢測資料竊取。

減少雲端接觸

Radware可以通過檢測混雜許可權並提供明智的強化建議幫助企業減少受攻擊範圍

檢測資料竊取活動

Radware採用先進的機器學習演算法識別雲帳戶中的異常活動，並針對資料竊取活動發出預警

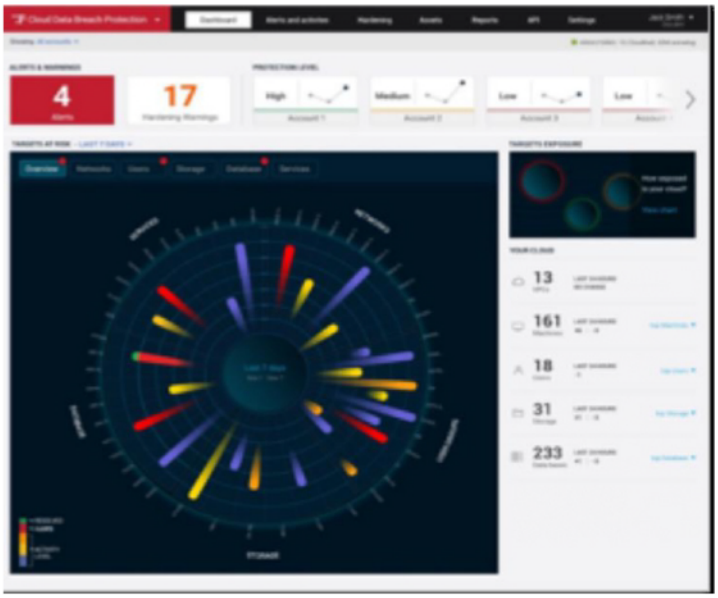
全面保護

雲端原生防護服務可以保護雲環境的整體安全態勢以及運行在其中的單個工作負載

雲端原生解決方案

雲端原生防護服務是無代理的雲端原生解決方案，可以實現低接觸率，部署時不會發生衝突，並且易於部署

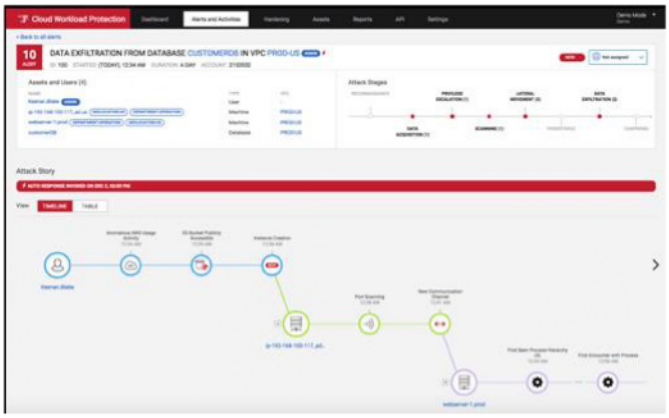
Radware如何確保您的工作負載和資料的安全



Radware 解決方案的主要優勢：

- 檢測公共資產
- 識別過多且異常的許可權
- 強化安全配置
- 發現資料竊取嘗試
- 自動化雲端安全功能
- 滿足合規需求

利用雲端原生防護服務保護您的工作負載



詳細的攻擊情節

Radware採用先進的機器學習演算法將單個事件關聯起來，並將其放置在具有情境的攻擊情節中，以便檢測潛在的資料竊取嘗試，並在其發展過程中加以攔截。

集中式安全管理

針對大量託管在雲端中的工作負載，Radware提供了集中的可見性和控制功能，可以幫助管理員瞭解何處發生了攻擊以及哪些資產受到了威脅。

具有情境感知的智慧強化

Radware可以通過分析已授權的許可權和使用中的許可權之間的差距，來檢測過多的許可權，並提供了智慧的強化建議來加強安全態勢並減少受攻擊範圍。

自動回應機制

Radware提供了內置方法，可以在檢測到可疑行為時自動修復這些行為，因此，在檢測到資料洩露時，您再也不會錯失良機。

無代理的非侵入性部署