雲端原生應用程式防護平台(CNAPP)

無代理雲端安全的先驅

Orca Security Platform 是業界領先的雲端安全平台，可辨識、確認優先等級並引導修復跨 AWS、Azure、Google Cloud、阿里雲等雲端平台、容器和 Kubernetes 的資產安全風險和合規問題。透過 Orca Security 解決方案，能以單一、完整的方式實現雲端環境100% 的覆蓋率和可見性。

Orca 改變雲端安全的專利技術-SideScanning ™，不需安裝任何代理程式，可直接從雲端配置和工作負載(workload)運作區塊儲存的頻外(out-of-band)收集資訊，進而對原本難以察覺的重大風險採取行動，包括漏洞、惡意軟體、錯誤配置、橫向移動風險、身分識別和存取管理(IAM)風險、錯置的敏感資料和API風險等。
所有資產相關資訊都可整合到單一平台中，透過Orca上下文感知引擎詳細了解 AWS、Azure和Google Cloud 等雲端環境中的資產風險，並讓資安團隊依據風險嚴重程度的排序，專注處理1%的重大關鍵問題。

Orca Security Platform 持續維持雲端合規性並提供漏洞管理、惡意軟體掃描和文件完整性監控等多種工具。Orca 支援40多個網路安全基準(CIS)和關鍵資產的合規框架，如 PCI-DSS、GDPR、NIST 和 SOC 2，並具有內建及自定模板，可滿足不同用戶的特定需求。

借助 Orca Security Platform 直觀且具彈性的查詢功能，每個用戶都可以快速搜尋雲端數據以獲取可用情報，同時也可透過整合的工作流程立即將問題分配給負責的團隊成員，以提高效率、加快修補速度，實現更好的投資報酬率。

雲端安全狀態管理 (CSPM)

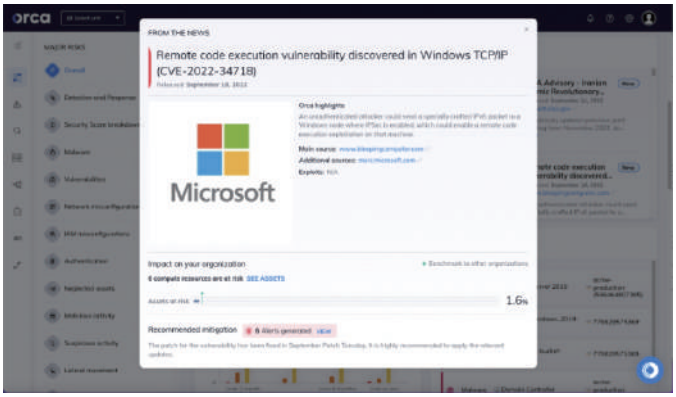
傳統的 CSPM 解決方案可幫助組織保持合規性並解決雲端風險，例如錯誤配置和過於寬鬆的身份驗證。但是，這僅涵蓋攻擊面一部分的風險，且將雲端工作負載、事件監控和機敏資料發現排除在外。
Orca 將雲端工作負載、配置、身份和權限安全、容器安全、機敏資料發現、檢測和回應整合到單一平台中，並橫跨整個生命開發周期(SDLC)。這讓 Orca Security Platform 能了解風險的前後脈絡，並識別看似無關的問題何時會產生危險的攻擊路徑。運用這些洞察，Orca 能有效確認風險的優先順序，確保資安團隊可以優先處理最關鍵的告警。此外，Orca 也會持續檢查多雲端資產中的錯誤配置，確保設置的安全性並遵守最佳實務及產業合規標準。

雲端工作負載保護平台 (CWPP)

與其他 CWPP 不同，Orca 不需安裝代理程式，可在幾分鐘內以 100% 的覆蓋率提供對雲端工作負載及雲端資產風險的可見性，並能橫跨雲端VM、容器、無伺服器應用程式、Kubernetes以及雲端基礎設施，而不影響效能和營運成本。此外，Orca還可掃描雲端配置和用戶身份，提供完整的上下文分析和告警優先排序。

雲端基礎設施授權管理 (CIEM)

Orca 將身份風險與其他風險數據（漏洞、錯誤配置、惡意軟體、機敏資料的儲存位置和橫向移動風險）結合起來，以幫助您優先考慮環境中的風險。若發現過於寬鬆的身份認證時會發出告警，並能根據潛在的業務影響進行風險優先排序。



雲端原生漏洞管理

Orca 為您的雲端環境建立完整漏洞清單，並結合20多個漏洞資訊來源，以發現、評估整個雲端資產中的漏洞。

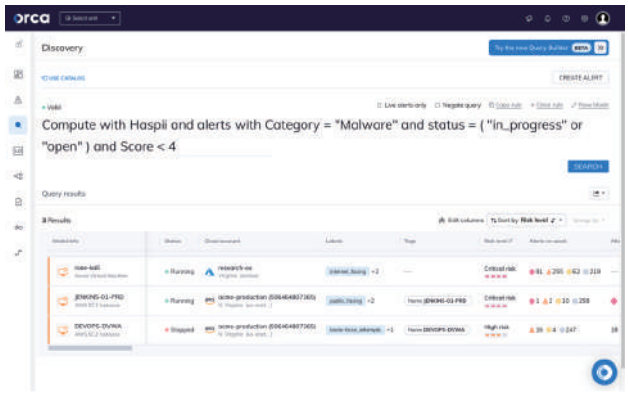
- 資產清單包含操作系統、應用程式、函式庫、版本和其他識別特徵的資訊。

- 將雲端資產的上下文、相關連接和風險分數納入評估，以評估須優先解決哪些漏洞。
- 如遇到 Log4Shell 等需要快速回應的問題，Orca 能快速識別易受攻擊的雲端資產，並優先修補會對營運構成最大風險的資產。

保護您的機敏資料

Orca 掃描雲端資產的每一處，搜尋有風險的機敏資料，從個人身份資訊 (PII) 到受保護的醫療保健資訊等。

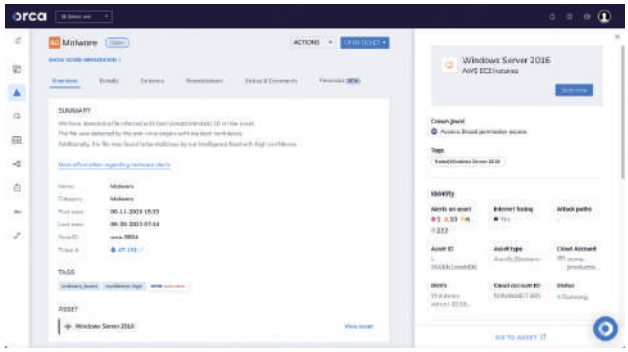
- 檢測雲端資產中每個工作負載內具風險的機敏資料，無論資產是運作中、閒置、暫停或停止狀態。
- 告警會指出機敏資料的確切位置，並提供遮罩樣本以進行有效的分類和修復。
- 機敏資料檢測含括各種個人身分資訊(PII)，如地址、Email信箱、信用卡號和身分證字號等。



檢測已知和未知的惡意軟體

Orca 將 SideScanning 結合多種惡意軟體檢測技術，以找出雲端工作負載和資源中的已知及潛在惡意程式碼。

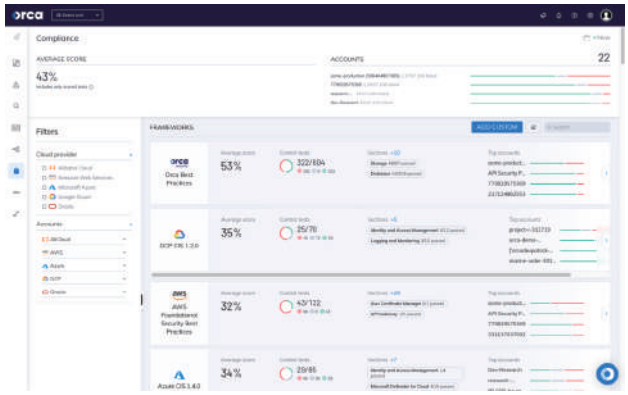
- 基於特徵碼的檔案hash(特徵)掃描 - 檢查已知的惡意軟體。
- 啟發式檔案分析(Heuristic file analysis) - 詳細檢查檔案以確定其用途、目標和意圖，進而標註是否為惡意軟體。
- 動態掃描 - 在受控制的虛擬環境中執行檔案以觀察其動向及表現是否為惡意軟體。
- 基因特徵碼偵測 - 比對過往的惡意軟體資訊以發現相同來源的惡意軟體。



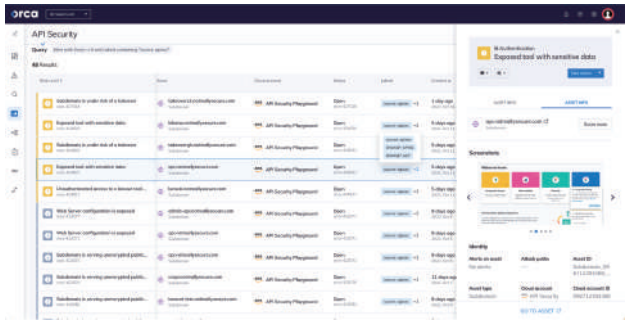
身份認證風險 - 集中式的多雲查找和合規

Orca 支援跨多個雲端平台，以追踪雲端資產、角色和權限，確保符合法規標準和網際網路安全性(CIS)基準。

- 獲得雲端中所有身份、配置、存取策略、權限和活動的精確上下文可見性。
- 查看所有雲端資產中的網路存取和公開資源。
- 提供20多個類別，1,300多項存取控制，包括身份驗證、資料保護、日誌記錄和監控、IAM錯誤配置及系統完整性。



API 風險優先排序及合規

Orca 掃描整個雲端資產並發現潛在危險的 API 安全風險，包括來自 OWASP API Security Top 10 告警，並提供可執行的資料和修補建議。

- 運用重要程度評分和基於上下文的資料（例如PII位置、API公開顯示等）排定風險的優先順序並加速修補行動。
- 藉由自動建議輕鬆識別 “不應暴露在外的資產” 。
- 採取預防措施來減少 API 攻擊面。搜尋與特定網域或子網域相關的風險，或特定期間內的告警。
- Orca提供帶連結的告警，高於稽核標準並遵守合規性架構（如PCI-DSS）。