雲端原生應用程式防護平台(CNAPP)

無代理雲端安全的先驅

Why Orca ?

- ✓ 單一平台、匯集多種雲端安全功能
- ✓ 只要幾分鐘，即可快速完成部署
- ✓ 100% 完整覆蓋所有雲端資產
- ✓ AI 驅動的雲端安全防護

Orca Security Platform 是業界領先的雲端安全平台，可識別、確認優先等級並修復跨 AWS、Azure、Google Cloud、阿里雲等雲端平台、容器和 Kubernetes 雲端資產安全風險和合規問題，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。

所有雲端資產資訊都能整合到單一平台中，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、身份及權限安全、容器安全、機敏資料查找、威脅偵測與回應，整合至單一平台中，並橫跨整個軟體開發生命週期（SDLC）。統一的安全架構讓 Orca 能掌握風險的前後脈絡，並識別出看似無關卻可能形成攻擊路徑的安全隱患。運用這些洞察，Orca 能有效確認風險的優先順序，避免告警疲勞，確保資安團隊可以聚焦處理最重要的威脅，提升整體防護效率。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 方案不同，Orca 採用無代理模式，可在幾分鐘內完成部署，並實現 100% 的完整覆蓋，提供雲端資產、雲端配置及雲端工作負載的風險可視性，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。

雲端弱點管理

Orca 為您的雲端環境建立完整弱點清單，並結合 20 多個弱點資訊來源，以發現、評估整個雲端資產中的弱點。

- 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。

資料安全態勢管理 (DSPM)

搜尋所有雲端資產的機敏資料、解決資料風險並遵守隱私法規。

- DSPM 儀表板為資安團隊提供雲端資料儲存、機敏資料及安全、合規性告警的資料可見性。
- 發現直接、間接的資料風險，讓資安團隊能採取預防措施來縮減資料攻擊面。
- 透過單一雲端安全平台驗證機敏資料的儲存是否符合監管框架、產業基準和隱私規範等資料合規性。
- 持續監控可能危及機敏資料的可疑活動，以便快速調查、分類潛在的資料外洩風險。

Orca CNAPP 解決方案

作為 CNAPP 集中管理平台，Orca 整合了多項重要解決方案，包括：

- ✓ **雲端安全態勢管理 (CSPM)**
- ✓ **雲端工作負載保護平台 (CWPP)**
- ✓ **雲端基礎設施權限管理 (CIEM)**
- ✓ **雲端弱點管理**
- ✓ **雲端容器及Kubernetes 安全防護**
- ✓ **資料安全態勢管理 (DSPM)**
- ✓ **API Security**
- ✓ **雲端偵測與回應 (CDR)**
- ✓ **多雲合規性 (Multi-cloud Compliance)**
- ✓ **左移安全 (Shift Left Security)**
- ✓ **雲端應用程式安全**
- ✓ **AI 安全態勢管理 (AI-SPM)**

檢測已知、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。

AI 安全態勢管理 (AI-SPM)

提供已部署 AI 模型 100% 的可見性，並防止資料篡改及外洩。

- 持續掃描整個雲端環境，並提供所有託管及非託管 AI 模型的完整視圖，包括各種影子 AI。
- 確保 AI 模型的配置安全，包含網路安全、資料保護、存取控制和 IAM 等，並提供自動及引導式修復以快速解決問題。
- 掃描、分類 AI 專案資料，若偵測到機敏資料，Orca 平台會發出告警，以便管理人員採取適當措施，防止資料外洩。
- 偵測 AI 服務及軟體中的金鑰和 token 是否在程式碼儲存庫中以不安全的方式暴露，並發出告警，以防止模型篡改及資料竊取。

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以加速修補行動。
- 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）。