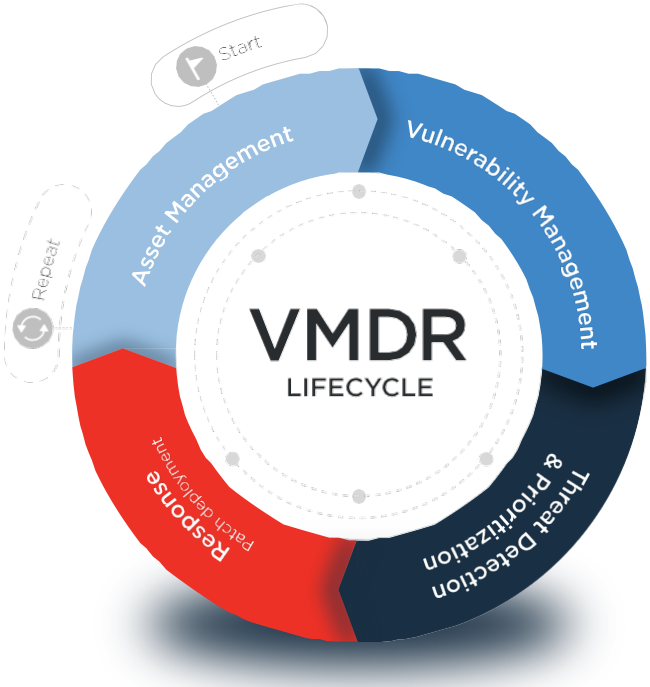
Qualys

Qualys VMDR® — 弱點管理、檢測和應變 多合一方案

將 #1 弱點管理解決方案提升到新的水平

在您的全球混合 IT 環境中即時搜尋、評估、確定優先級別與修補重大弱點 — 全部來自單一解決方案。



VMDR 內建協作功能

識別所有在全球混合 IT 環境內已知與未知資產

清楚知道全球混合 IT 環境中的活動是安全的基礎。 自動搜尋所有位於各地的已知和未知 IT 資產，以獲得一個完整的分類清單，其中包含供應商生命週期資訊與其他詳細資訊。

以六個標準差等級精確度來分析弱點和錯誤設定

自動偵測資產內每個以 CIS 基準區分的漏洞和錯誤設定嚴重等級。

快速聚焦於最緊急的事情

使用進階關聯和機器學習，自動優先處理最關鍵資產上最高風險的弱點，將數千個弱點減少到幾百個。

讓您的資產免受於遭受嚴重的威脅

透過按一鍵修正功能，即可部署最相關的修正程式，以達到快速修復任何規模環境中的弱點和威脅。

今時今日的流程需要許多不同的團隊協作，使用多點解決方案將會 — 增加了許多關鍵修補流程的複雜性與時間。

使用多個傳統的端點解決方案並不能很好地相互協作，也因此造成了令人頭痛的整合問題、誤報問題和延遲問題。最終造成的結果是什麼？設備沒識別到，關鍵資產被錯誤分類，弱點優先級別錯置，修補程式沒有完全部署。

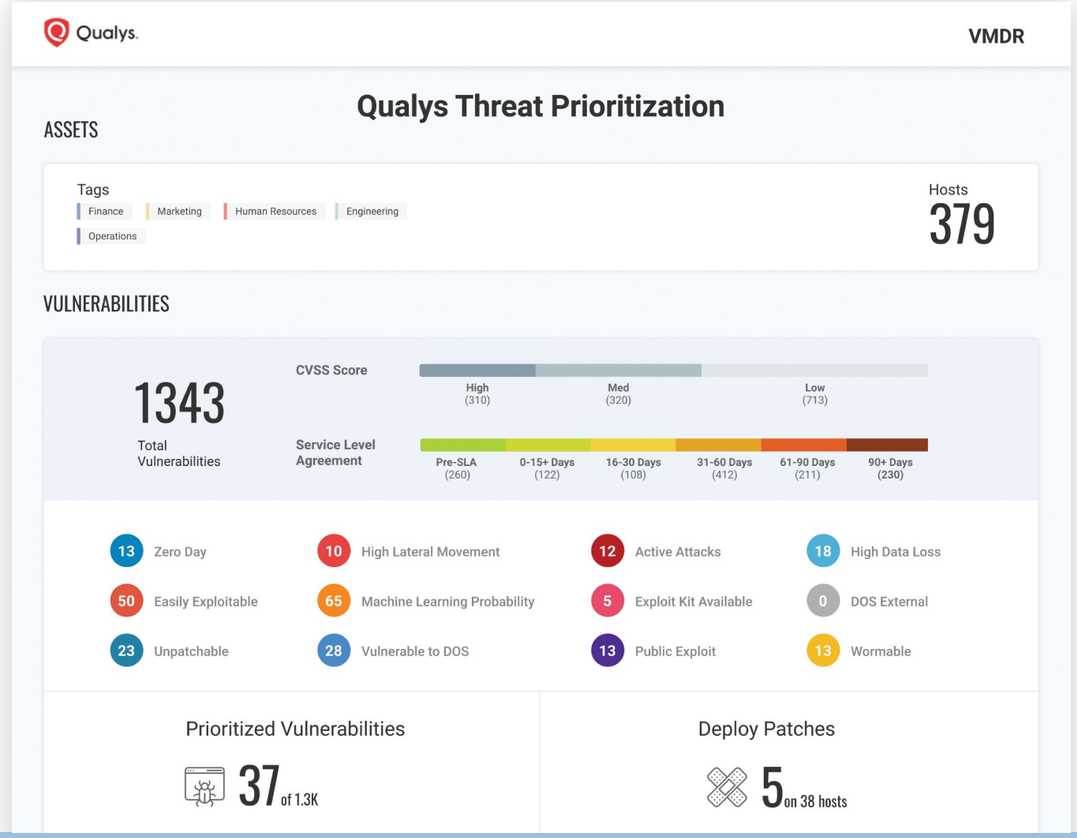
用於搜尋、評估、偵測和回應的單一應用程式。

Qualys 雲平台結合其強大且輕量化的 Cloud Agents、Virtual Scanners 和 Network Analysis（被動掃描）功能，將弱點管理程式的所有四個關鍵應用整合到一個強大且有用處的應用程式中來編排工作流程。

Qualys VMDR® 使組織能夠自動搜尋其環境中的每一個資產，包括出現在網路上的非託管資產，清點所有硬體和軟體，並對關鍵資產進行分類和標記。 VMDR 持續評估這些資產的最新漏洞，並應用最新的威脅情報分析來確定可被利用的弱點的優先級。最後，VMDR 會自動檢測易受攻擊資產的最新替代修正程式，並輕鬆部署它以進行修復。

內建編排協作功能

透過在單個應用程式工作流程中提供所有這些，VMDR 使整個過程自動化，並明顯提高組織應對威脅的能力，來達到防止可能的漏洞利用。



Key Benefits

純雲端架構
不需要部署多餘的硬體設備。一切都在雲端，隨叫隨到，隨時可以開始運行。

部署簡單
部署非常簡單。借助不限數量的虛擬掃描器，讓您可以任何時刻隨時啟動掃描器。

包含 VM
VMDR 擁有您熟悉和信任的相同漏洞管理解決方案，以及許多其他出色的應用程式。

大幅減少時間和金錢
使用單個雲平台可以節省大量資源和安裝多個代理程式、多個控制台和整合相關資源所需的時間。

1
資產管理
自動化資產識別與分類
清楚知道全球混合 IT 環境中的活動是安全的基礎。 VMDR 使客戶能夠自動搜尋和分類已與和未知資產，持續識別未納入管理的資產，並建立自動化工作流程以有效管理它們。
收集資訊後，客戶可以即時查詢資產以及任何相關資訊，以了解硬體、 軟體、系統配置、應用程式、服務、網路資訊等更多深入資訊。

2
弱點管理
即時漏洞和錯誤設定偵測
VMDR 使客戶能夠根據 CIS 基準來將資產自動偵測漏洞和嚴重的錯誤設定分類。
錯誤設定會導致違規與失去合規性，因而在沒有常見弱點和暴露 (CVE) 的資產上產生漏洞。
VMDR 持續識別最廣泛的業界設備、操作系統和應用程式上的關鍵弱點和錯誤設定。

3
威脅分級
自動修復優先級別
VMDR 使用即時威脅情報和機器學習模型來自動判斷最關鍵資產上風險最高的漏洞的優先級別。可利用、主動攻擊和橫向移動等指標會利用當前存在風險的弱點，而機器學習模型則明白顯示最有可能成為嚴重威脅的弱點，從而提供多個等級的優先級別排序。

4
修補管理
迅速完成修補和修復
在按風險對漏洞進行優先級排序後，VMDR 透過部署最相關的修補程式，在任何規模的環境中快速修復目標弱點。 此外，基於策略的自動化流程重複作業使系統保持最新狀態，為安全和非安全修補程式提供主動修補程式管理。這大大幫助減少了維運團隊在減少弱點修補流程內必須持續追蹤弱點修補狀況的時間。

確認與重複
VMDR 從單一管理平台完成弱點管理生命週期並停止循環，該管理平台具有趨勢走向與即時顯示的儀表板且可客製化和小部件。
VMDR 按資產定價，無需更新軟體，可顯著降低您的總擁有成本。

Qualys VMDR® — 多合一解決方案

		內含	另加功能
資產管理			
資產搜尋	檢測和清點連接到全球混合 IT 環境的所有已知和未知資產，包括本地端設備和應用程式、移動設備、端點、雲端、容器、OT 和 IoT。包括 Qualys 被動掃描傳感器。	○	
資產管理 獲取所有 IT 資產的最新即時資產管理資訊	• **本地端設備資產管理** – 偵測連接到網路的所有設備和應用程式，包括伺服器、資料庫、工作站、路由器、印表機、物聯網設備等。 證書資產管理 – 偵測和編目來自任何證書頒發機構的所有 TLS/SSL 數位證書（內部使用和外部使用）。 • **雲端資產管理** – 監控用戶、instance、網路、儲存相關、資料庫及其關係，以持續獲取跨所有公有雲平台的資源和資產的清單。 • **容器(Container)資產管理** – 發現和追蹤容器主機及其資訊——從開始到運行。 • **行動裝置資產管理** – 偵測和編目整個企業的 Android、iOS/iPadOS 設備，並提供有關設備、其設定和已安裝應用程式的大量資訊。	○	
資產分級與標準化	收集詳細信息，例如資產的詳細信息、正在運行的服務、已安裝的軟件等。消除產品和供應商名稱的變化，並按所有資產的產品系列對它們進行分類.	○	
豐富的資產訊息	取得進階、深入的詳細資訊，包括硬體/軟體生命週期 (EOL/EOS)、軟體授權稽核、商業和開源授權等。		○
CMDB 同步	在 Qualys 和 ServiceNow CMDB 之間雙向同步資產資訊。		○
弱點管理			
弱點管理	Qualys 是 VM 偵測方面的市場領導者。我們提供您最全面的signature資料庫，在最廣泛的資產類別中持續檢測軟體弱點。	○	
設定評估	根據互聯網安全中心 (CIS) 基準來實施評估、報告和監控與安全相關的錯誤設定問題。	○	
證書評估	評估您的數位證書（內部使用和外部使用）和 TLS 配置的證書問題和弱點	○	
附加評估附加組件	• **行動裝置弱點與錯誤設定安全評估** – 持續偵測設備、操作系統、應用程式和網路漏洞並監控關鍵的行動設備設定。 • **雲端安全評估** – 持續監控和評估您的 PaaS/IaaS 資源是否存在設定錯誤與非標準部署。 • **容器安全評估**– 掃描您環境中的容器映像檔和正在運行的容器，以查找高嚴重等級的漏洞、未經批准的軟體並推動修復工作。包含在構建階段使用 CI/CD 工具和註冊表plugins進行偵測的能力。		○
威脅偵測與分級			
持續監測	即時提醒您網路異常情況。透過識別威脅並監控意外的網路變化，以防它們變成漏洞。	○	
威脅保護	找出最關鍵的威脅並優先修補。使用即時威脅情報和機器學習，控制不斷進化的威脅，並確定最先要修復的內容。	○	
應變處理			
修補程式偵測	自動關聯特定主機的弱點和修補程式，縮短修復時間。搜索 CVE 並確定是最新的修補程式。	○	
Qualys Cloud Agents 修補管理	透過使用 Qualys Cloud Agents 消除對第三方修補程式部署解決方案的依賴，加快修補程式部署。		○
行動裝置修補管理	卸載或更新有弱點版本的應用程式、提醒用戶、重置或鎖定設備、更改密碼等。		○
Container Runtime 安全	透過細緻化的行為策略部署，在傳統的基於主機的容器還有容器即服務的環境中保護和監控正在運行的容器。		○
證書更新	透過 Qualys直接更新即將到期的證書.		○

VMDR 還包括了無限制數量的：Qualys 虛擬被動掃描傳感器（用於搜尋）、Qualys 虛擬掃描器、Qualys 雲端代理程式、Qualys 容器傳感器和用於網路頻寬優化的 Qualys 虛擬雲代理閘道器傳感器。