Qualys 雲平台

一切可見，一切安全

Qualys 雲平台可讓您對全球 IT、安全及合規狀態進行持續、always-on 的評估，並能在 2 秒內查看所有 IT 資產，無論它們位於何處。透過自動化的內建威脅排序、修補和其他回應功能，提供用戶一個完整的點到點安全解決方案。

Qualys 創新的雲端架構，為您的資訊安全和合規需求提供快速部署、易於擴充、實時防護，且不需硬體設備的解決方案，無論是機房端設備、容器、雲端服務或移動終端，都能透過單一平台進行實時管理與分析。

在本地端、終端、移動設備、容器或雲端環境中，Qualys 雲平台的感測器(Sensor)會保持 always-on 的狀態，讓您能在 2 秒內連續查看所有 IT 資產。感測器提供硬體、虛擬設備或代理程式(Agent)版本，可遠端部署、集中管理及自動更新。

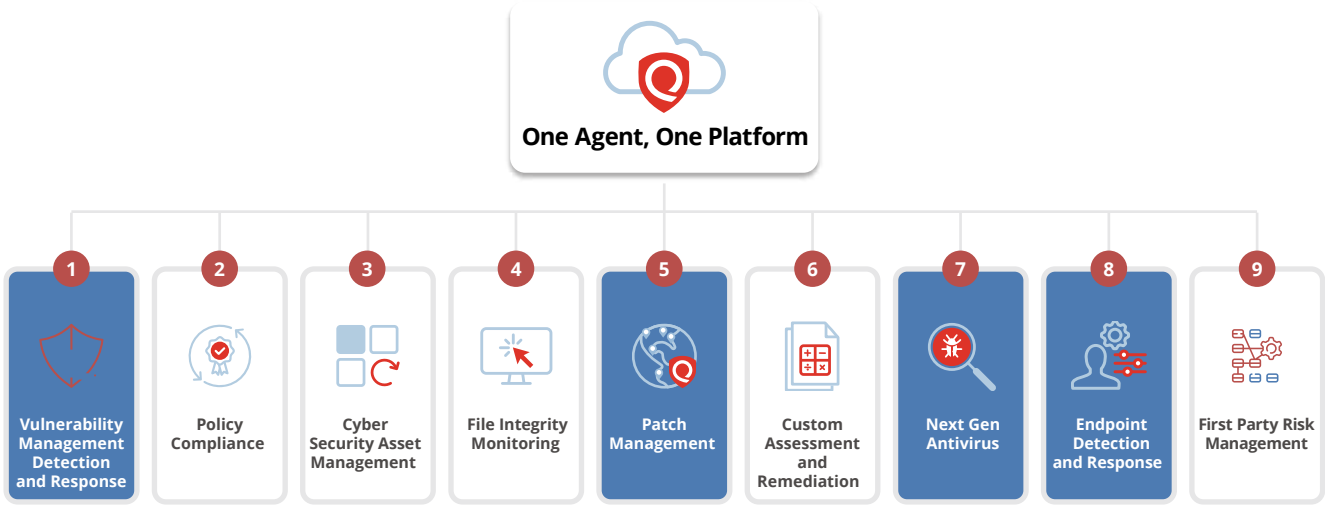
Qualys 雲平台優勢

- 不需添購、管理硬體設備
- 降低營運成本
- 易於執行分散式站點及網段的掃描
- 滿足快速擴充的需求
- 實時進行資訊更新
- 漏洞資訊經過層層加密保護

Qualys 雲平台可直接以 Web 瀏覽器操作，不需安裝任何軟體。強大的儀表板方便在單一畫面中檢視各式統計數據，並可依需求提供儀表板客製化編排。

Qualys 在全球 130 多個國家擁有 11,000 多個客戶，包括富比士全球 100 大及財富 100 強中的大多數公司。

Qualys 幫助企業在單一平台上簡化並整合他們的安全與合規解決方案，將安全納入數位轉型計畫中，以提升資訊敏捷性、強化業務成效並節省大量成本。



Qualys 雲平台提供多種安全防護

為強化您的資訊安全資產管理與合規需求，Qualys 提供以下功能模組：

Asset Management 資產管理

CASM網路安全資產管理

查看整個攻擊面，持續維護您的 CMDB (配置管理資料庫)，並追蹤 EOL/EOS 軟體

EASM 外部攻擊面管理-New

從攻擊者視角持續查找面向互聯網的資產與未經授權的軟體，並快速進行修復，實現可見性與風險追蹤

Vulnerability & Configuration Management 弱點及配置管理

VMDR 弱點管理、檢測與回應

讓 IT 資產環境中的發現、評估、優先排序和漏洞修補效率提升 50% 以上

ETM 企業 TruRisk 管理平台-New

整合第三方工具的安全與漏洞資訊，將網路風險的衡量、管理、緩解集中至單一平台

WAS 網頁應用程式掃描

透過 Shift left DAST (動態應用程式安全測試) 在 CI/CD 環境中自動掃描

CWP 雲端 workload 防護

掃描、排序並修復雲端環境裡 VM、容器和無伺服器 workload 的漏洞

CS 容器安全

發現、追蹤並持續保護容器從建置到實際運行時的安全

Risk Remediation 風險修復

PM Patch 管理

簡化並加速 IT 資產弱點與 Patch 的關聯性管理

CAR 客製化評估與修復

提供可快速建立的客製化自動工作流程腳本及控件，以實現企業所需的安全性及合規性

Threat Detection & Response 威脅偵測與回應

EDR 多向量端點偵測與回應

進階端點威脅防護、優化的威脅上下文資訊及告警排序

XDR 上下文關聯延伸偵測及回應

將偵測和回應擴展到企業端點之外

Compliance 合規管理

PC政策合規

評估網路 IT 系統的安全配置，降低風險，輕鬆遵循內部政策和外部規範

FIM檔案完整性監控

記錄、追蹤全球 IT 系統的檔案變更，減少告警並保護檔案免於惡意用戶和網路威脅侵害

Cloud Security 雲端安全

Total Cloud CNAPP 雲端原生應用防護平台

發現、評估、優先排序、防禦和修復多雲環境的漏洞、威脅和錯誤配置

CSPM 雲端安全狀態管理

提供公有雲 workload 和基礎設施的統整清單，可持續發現、監控、分析雲端資產是否有錯誤配置和非標準部署

IaC 基礎設施即程式碼安全

偵測並修復 IaC 範本中的安全性問題，以消除雲端基礎設施的潛在安全威脅

SSPM SaaS 安全態勢管理-New

管理整個 SaaS 應用程式堆疊 (stack) 的安全狀況及風險

CWP 雲端 workload 防護

掃描、排序並修復雲端環境裡 VM、容器和無伺服器 workload 的漏洞

CDR 雲端偵測與回應

結合人工智慧和深度學習演算法進行實時多雲威脅偵測，持續保護多雲環境免受主動利用 (active exploitation)、惡意軟體和未知威脅。

CS容器安全

發現、追蹤並持續保護容器從建置到實際運行時的安全

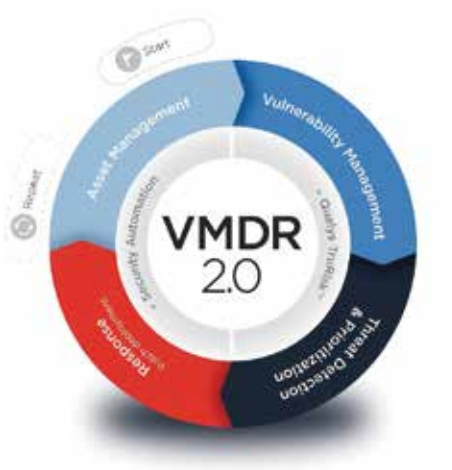
VMDR 2.0 with TruRisk™ 全方位弱點管理、檢測和回應

透過單一管理介面，實時發現、評估、確認優先順序並修補重要漏洞

風險成長的速度超出了傳統 VM 和 SIEM 工具的管理能力。資安與 IT 團隊需要新的方法來因應網路威脅，清楚掌握網路安全風險並自動化工作流程以實現快速回應。

借助 VMDR，企業能獲得對網路風險的可見性和洞察力，進而根據風險確認資產或資產群組的弱點優先順序。安全團隊可以採取行動來降低風險，幫助企業衡量其真實風險，並隨時間追蹤風險降低的情況。

Qualys VMDR 2.0 提供基於風險的弱點管理解決方案，根據風險和業務關鍵性對漏洞和資產進行優先排序，確定漏洞、錯誤配置和資產的優先處理等級，透過大規模修復漏洞來降低風險，並透過時間追踪幫助組織衡量安全防護的有效性。Qualys VMDR 2.0 還與 ServiceNow 等資訊服務管理系統整合，實現點到點弱點管理的自動化和運作。



了解、管理網路安全風險
使用 Qualys TruRisk ™ 量化漏洞和資產的風險，幫助組織主動降低風險並追踪風險隨時間降低的情況。

使用無程式碼工作流程自動修復
透過 Qualys Flow 實現弱點管理和修補的操作任務自動化與編排，以節省寶貴的時間。

防止攻擊持續發生
Qualys 威脅資料庫整合來自 25 個來源以上的 18 萬個漏洞分析，提供對潛在攻擊的預先告警。

識別環境中的所有資產
檢測所有 IT、OT 和 IoT 資產，提供完整且分門別類的資產清單，並包含供應鏈生命週期資訊等詳細訊息。

以 6 sigma 的準確度分析漏洞和錯誤配置
根據互聯網安全中心(CIS)基準，自動檢測資產漏洞和重大錯誤配置。

快速且大規模的修復威脅
與 ServiceNow、JIRA 等資訊服務管理系統(ITSM)整合，自動分配案件並啟用修復排程以降低平均修復時間(MTTR)。

資產管理 - 自動資產識別與分類

VMDR 讓用戶能自動發現已知和未知資產並對其進行分類，持續辨識未託管資產，並建立自動化工作流程以有效進行管理。完成資料收集後，用戶可以立即查詢資產和相關屬性，以深入了解硬體、系統配置應用程式、服務、網路資訊等。

弱點管理 - 即時偵測漏洞及錯誤配置

VMDR 可讓用戶根據 CIS 基準自動偵測資產的弱點和嚴重錯誤配置。藉由 Qualys 對 86,000 以上個漏洞的支援以及對 CIS 基準的全面覆蓋，組織可以更快地回應威脅。VMDR 與 TruRisk 持續識別 IT 環境面臨的重大風險，包含業界廣泛使用的裝置、作業系統和應用程式上之關鍵漏洞及錯誤配置。

威脅優先排序 - 根據風險自動排定弱點修復順序

VMDR 運用即時威脅情報、進階關聯和強大的機器學習模型，自動對關鍵資產上風險最高的弱點進行排序，並透過對每項資產的業務影響評估，進一步確認修復的優先順序。

修復管理 - 修補（Patch）與修復（Remediation）唾手可得

在依風險對弱點進行優先排序後，VMDR 整合相關 Patch 資源，在不同規模的環境中快速修復目標弱點。此外，基於策略的自動化作業可讓系統保持最新狀態，為安全性和非安全性 Patch 提供主動式管理。

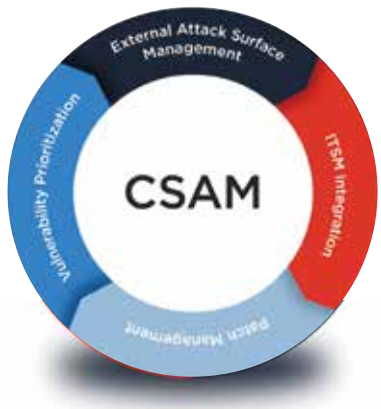
CSAM 網路資安資產管理 (含外部攻擊面管理)

以駭客視角檢視您的攻擊面

傳統攻擊面管理和弱點管理解決方案難以看見現今駭客所瞄準的外部資產和軟體全貌。為了降低網路風險並整合資安差距，必須實現內外部面向互聯網資產的完全可見性。

攻擊面正急速擴大，為攻擊者提供了新的目標。超過 30% 的地端、雲端資產和服務未進行盤點，這是網路安全可見性的巨大落差！

網路安全資產管理 (CSAM) 是 Qualys 一項雲端服務，能像攻擊者一樣查看您的攻擊面，並整合資安與 IT 的資產管理。CSAM 可以持續發現、分類、修復和改善其內部和外部 IT 資產的網路安全狀況，同時查找所有已知和未知、面向互聯網的資產，以實現 100% 的可見性和風險追蹤。



Qualys CSAM 2.0 包括外部攻擊面管理，增加了“縱深防禦”以更新組織的網路安全狀態。CSAM 2.0 透過具有紅隊型態的資產及漏洞管理解決方案，提供持續發現、分類未知資產的能力，以實現 360 度的全面性涵蓋。

特色與效益

基於風險的網路安全建立在攻擊面管理（ASM）基礎上。透過網路安全資產管理（CSAM），資安和 IT 營運人員可以獲得攻擊者和防禦者對其環境全面、完整的可視性，包括資產、資產群組、網域、子網域、生命週期（EOL/EOS）等。結合外部攻擊面管理（EASM），CSAM 可以幫助組織發現、偵測、確認資產風險的優先順序，並編排資安和 IT 團隊之間的工作流程，以消除作業摩擦、改善修復成效並降低網路風險。

透過統一的盤點和資產目錄（包括第三方資產情資以及內對外與外對內的數據）來降低網路風險。

透過 EOL/EOS 盤點、未經授權軟體查找和關鍵 agent 覆蓋等功能，找出資安弱點並監控資產運作狀況。

透過本機整合的工作流程簡化、改善弱點管理、AppSec 和 Patch 管理程式。

透過與 ITSM、CMDB 和 Ticket Tool 的雙向整合，提升 90% Patch 速度，更快完成事件處理。

Qualys

Web Application Scanning 網站弱點掃描服務

查找、修復網站應用程式與 API 弱點

Qualys 雲平台提供針對網站應用程式的弱點掃描及錯誤配置管理服務，可直接透過雲端服務，快速、方便完成佈署準備。立即管理您的網站資產、掃描弱點與錯誤配置、修復追蹤，並透過惡意軟體掃描，讓網站更加安全，且無需花費建置任何硬體設備。

WAS 掃描企業的網站並識別、報告感染的情況，如經過行為分析找出的零時威脅。詳細的惡意軟體感染報告內也包含了須修復的程式碼。中控儀表板可顯示掃描活動、受感染頁面和惡意軟體感染趨勢，並允許用戶直接從介面採取行動。惡意軟體檢測功能為選用的附加模組。

- **全面查找**

  搜尋企業內存在的網站，建立網站資產清單。

  Qualys WAS 透過查找整個網路後可得到的資訊包括：

  - 已確認及未確認的網站
  - 可使用標籤或群組方式管理網站資產

  分類弱點風險等級，讓資安人員優先修復重要問題。

- **深入掃描**

  WAS 的動態深度掃描涵蓋邊界、內部環境和正在開發中的所有應用程式，並可支援移動設備的 API。WAS 還涵蓋公有雲實例，為您提供 SQLi 和 XSS 等弱點的即時可見性。

  透過深入、完整、精確的掃描查找網站弱點，並以近趨於零的誤報率保護您的網站應用程式。可漸進式逐步掃描並繞過阻擋掃描整個應用程式的限制。

- **DevOps 安全工具**

  WAS 可提升 DevOps 環境中應用程式開發和部署的安全性，檢測程式碼安全問題、測試品量保證(Quality Assurance)並產出統整報告。WAS 也與 Qualys WAF 高度整合，可持續監控並虛擬修補應用程式，快速防禦尚未修復的弱點。

  檢測 OWASP Top 10 風險，如 SQL 注入、跨站腳本(XSS)、跨站請求偽造 (CSRF) 和無效重定向等。

  可檢測具身分認證的網站應用程式，還可用自動執行腳本的方式登入系統，擴大掃描覆蓋率。

- **惡意軟體檢測**

  可手動執行掃描，亦可透過排程自動執行網站掃描，確認是否受惡意軟體感染。

PCI Compliance & SAQ PCI 合規掃描與自我審查評估表模板

簡單、快速、自動化完成 PCI 合規檢查

Qualys PCI 政策合規提供企業、網路商家和服務供應商最簡單、最具成本效益和高度自動化的方式來實現PCI DSS (信用卡行業資料安全標準)合規性。

除了以 PCI ASV 進行掃描外，透過完整的 Qualys PCI 合規解決方案，更能滿足 97% 以上的 PCI DSS 要求。在資產管理、弱點檢測和回應、支付網站應用程式安全、安全配置管理和安全評估問卷等方面，都能獲得安全性和合規性。

PCI DSS 要求企業每 90 天要對所有面向 Internet 的網路和系統執行一次有既定流程的網路安全掃描。為實現合規性，企業必須識別、修復在掃描過程中檢測到的所有重大弱點。

Qualys PCI ASV 應用程式提供：

- 自動化並大幅簡化的掃描與修復流程
- 易於使用的 PCI DSS 合規弱點掃描報告
- 透過 Qualys 雲平台準確掃描弱點
- 為每個檢測到的弱點提供詳細說明，並提供驗證過的修補連結以進行快速修復。

當您完成各項驗證操作後，Qualys PCI ASV 應用程式可透過以下兩種模式執行 “自動提交” 功能，完成合規流程：

√ 自動將合規報告直接提交給收單銀行

√ 可下載 PDF 格式的 PCI 合規報告再另行提交給收單銀行

可加購自我審查評估表模板(SAQ)，內含多種合規所需的自我審查評估表，包含 ISO、PCI-DSS、HIPAA、NIST、GDPR 等各種法規型式及版本的模板。PCI 審查評估表提供直接填寫問卷並寄發給收單銀行或下載 PDF 格式報告兩種模式。