

全方位

弱點管理最佳平台

A Unified View of Your Security & Compliance

自動化弱點管理及智慧型工作流程整合解決方案



弱點管理



網頁應用程式



政策合規



QUALYS[®]
ON DEMAND SECURITY



- ? 我有多少IT資產?
- ? 網頁防火牆防禦政策是否設定OK?
- ? 我要如何修正弱點?
- ? 我目前的資安狀況是否處於高風險狀態?
- ? 每部電腦有多少弱點呢?
- ? 目前多少電腦符合政策規範?
- ? 什麼弱點會瓦解我的IT環境?
- ? 這些弱點是否會導致企業資料外洩?

QualysGurad是您全方位弱點管理的最佳平台



VM

弱點管理

Vulnerability Management

適合全球佈署及具備安全風險和安全弱點管理

WAS

網頁應用程式弱點掃描

Web Application Scanning

自動化檢測網頁應用程序之安全性

MDS

網頁應用程式惡意程式偵測

Malware Detection Service

自動化檢測網頁應用程式是否具備惡意程式或惡意連結

PC

政策合規

Policy Compliance

定義、審核和記錄IT安全合規性

PCI

PCI政策合規

PCI Compliance

自動化評估檢測是安全政策否合於PCI規範



Qualys安全認證 Qualys安全認證向來訪的使用者展示您的網站經過嚴格的安全檢驗，讓使用您的網站的使用者可以安心使用。



Vulnerability Management

弱點管理

QualysGuard® 弱點管理具備完整的自動化弱點管理機制，首先可透過網路探勘功能可以迅速了解企業內部 IT 資產狀況，在透過 IT 資產優先排序、漏洞評估報告和弱點修補措施等功能。QualysGuard 為提供完整的安全弱點知識庫，可以為使用者提供最新病毒和安全威脅的持續性防護。

使用 QualysGuard 弱點管理，從小型企業到大型企業均可透過集中式報告、提供您完整的弱點修補順序，有效地進行管理和控制。QualysGuard 提供詳細的安全漏洞報告，其中包括嚴重程度進行排序，讓您清楚了解如何進行修補計畫，尚可對於安全問題做長期的觀察及統計進行趨勢分析報告，讓您充分掌握企業資訊安全。





探勘您的網路環境

首先透過網路探勘的功能快速的了解您整體網路架構及網路設備。QualysGuard 的掃描技術具有非侵入式而且準確性高。QualysGuard 弱點管理可以發現所有的網路設備和應用程式執行程序，包括 PC、Server、作業系統、應用程式執行程序、路由器、行動裝置、無限設備等。



管理您的網路資產

根據您的需要自行定義企業資產風險加權計分機制，可從低到高有五個等級之加權計分系統，企業可依照此資產對於業務營運的重要性進行加權計分，如此所產具的報告可協助您定義弱點修補計畫之修補參考依據。



識別弱點

具備業界最大、最新的安全漏洞檢測資料庫，QualysGuard 的外部和內部掃描器 (Scanner) 可以精準地檢測您整個網路中存在的漏洞。每週新的弱點更新說明文件至使用者，使用者可隨時掌握最新的威脅資訊。

Patch Report		
Total Patches	Hosts Requiring Patches	Vulnerabilities addressed
2,110	71	8,853

強大的威脅分析報告

直觀且易於閱讀的報告，可同時提高層長官所需摘要分析報告和技術人員需要了解的詳細技術分析報告。Qualys 鉅細靡遺的針對每個漏洞詳細的說明，其中包括，安全威脅分析，若漏洞倍利用的後果以及針對此漏洞提供對應的解決方案。



滲透測試參考訊息

在您進行弱點評估期間，提供客戶此弱點相關安全資訊的引用。有了這個功能，可查看遊第三方單位提供最新相關弱點是否可進行滲透測試的說明，您可以使用由第三方廠商所提供的滲透測試工具，進行此弱點的驗證，來確認此弱點之有效性。



Zero-Day 威脅分析

Zero-Day 威脅分析服務，讓您最新的資安威脅，透過它您可以提前了解這些新的資安威脅對您 IT 環境有哪些影響。

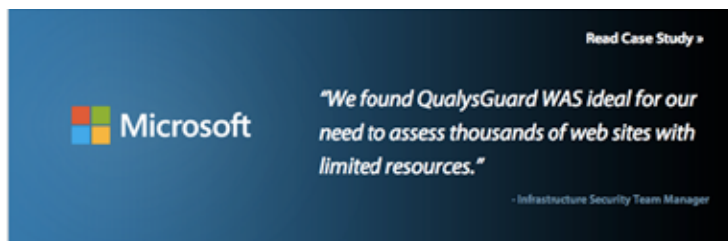


Web Application Scanning

網站應用程式掃描及
惡意程式偵測

QualysGuard 網站應用程式掃描提供您最佳的防禦措施

- Identify OWASP Top 10 Risks
- Complete Web Security with WAF Integration
- No software to install, no upfront investments
- No ongoing maintenance
- Scale seamlessly from a handful of apps to thousands



提供您最專業的掃描報告

OWASP(Open Web Application Security Project) 所列 10 強名單已經成為網站應用程式，最常遇到的問題將其分類，並成為網頁應用程式弱點參考的依據。QualysGuard WAS 讓您精準地找到這些漏洞，例如：SQL Injection、Cross-Site Scription、Cross-Site request forgery 及 URL redirection 等並學習如何有效地消除它們。



協助您找到網頁深處的惡意程式

維護網站信譽是目前企業一個重要的課題，因為網站往往代表了一個企業的形象，別讓駭客再您的網站植入一些惡意程式或惡意程式碼。QualysGuard MDS 透過先進的行為分析技術，有效地識別隱藏於您網站之中的惡意程式或間諜程式，以增加網站的安全性。



完整 API 擴充功能

我們提供豐富且多樣化的 API 讓您使用我們的產品可以輕鬆的與其他資安的產品整合，您可以使用 QualysGuard WAS 網頁弱點掃描之功能，將掃描的結果匯入網頁應用程式防火牆 WAF(Web Application Firewall) 並建立安全的防禦政策，讓您減少管理的時間而且大幅增加防禦政策的正確性及有效性。不僅僅如何我們還可以跟您企業之中的事件管理平台 (SIEM) 和企業風險管理 (ERM) 整合，以增加整體資訊安全強度。



高度客製化報表系統

把您的掃描結果，透過簡單的幾個步驟及互動式報表產出功能，您可以執行功能強大的分析，也可透過內建的報表範本功能，輕易的產出您想要的報表呈現方式。



Policy Compliance

政策合規檢測

IT 安全、稽核和合規性，Qualys 團隊在幫助企業符合多個法規並滿足內部和外部稽核機構的要求時，一直面臨較大的壓力。此外，許多法規都針對 IT 環境完整性和安全性方面的要求。

使用 QualysGuard 政策合規性 (Policy Compliance)，組織不僅能降低內部和外部威脅的風險，同時還可以通過多種合規性方案提供審核人員要求的合規性憑證。QualysGuard PC 提供高效的自動化工作流程，允許 IT 安全和合規性專業人員：

- 定義政策，描述組織如何提供安全性和完整性。
- 提供記錄，證明已實施這些政策。
- 提供記錄憑證，說明組織已發現和修復任何策略遵從性問題。



自行定義合規政策

您可以自行定義企業合規的政策也可以透過內建國際資安政策來稽核企業內部或外部系統。這些政策基於 CobIT、SOX、HIPAA 等熱門的合規性標準。Policy Library 是一個集中式技術控制平台，用以針對多種標準和技術（操作系統和應用程序）進行合規性檢測，Qualys 能夠支援下列系統平台：

- Technologies: AIX 5.x, HP-UX 11.x, Linux Red Hat Enterprise 3, 4, & 5, Oracle 9i, 10g and 11g, Solaris 9.x, Windows 2003 Server and Windows XP desktop...
- Frameworks: COBIT 4.0, ISO 17799, NIST SP800-53...
- Benchmarks: CIS (member info, certifications)
- Compliance Regulations: SOX 404, GLBA, HIPAA, Basel II...



合規檢測報告

直觀、易於閱讀的報告提供對合規情況的詳細技術分析、執行級別摘要和專為審核人員定制的報告。自定義自己的報告，或使用基於下列模板的交互式報告：

- 策略報告，提供對特定策略的詳細遵從情況。
- 身份驗證報告，識別身份驗證的通過或未通過狀態。
- 個別主機報告，識別特定主機的合規情況。
- 控制通過 / 未通過報告，識別特定控制的通過 / 未通過狀態



PCI Compliance

PCI 政策合規

QualysGuard® 合規性 (PCI) 為企業、在線商家和會員服務提供商提供了符合銀行業數據安全標準的方法，該方法具有簡單、性價比高且高度自動化的特性。PCI DSS 為組織提供了用以確保信用卡持卡人信息安全、避免出現安全漏洞所需的規範。QualysGuard PCI 具備高精度掃描架構和技術，QualysGuard 已被全球數千家組織使用，來消除可能招致網絡攻擊的安全漏洞。



PCI 合規狀態顯示

借助 QualysGuard PCI，實現 PCI 合規性狀態將變得輕而易舉，同時還可確保網路的高度安全性。QualysGuard PCI Web 應用程序可為你提供漸進式簡易操作方法和合規性提示，使您輕鬆實現 PCI 合規性。



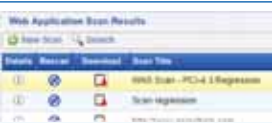
詳細的修補說明快速消除安全威脅

PCI DSS 還要求企業對 Internet 的網路和系統每 90 天執行一次網路安全掃描。要實現合規性，企業必須識別掃描期間所檢測到的各項重大安全漏洞並採取修補措施。QualysGuard PCI 通過提供易於使用的漏洞（可導致無法通過 PCI DSS）報告和識別功能，將原本異常繁瑣的過程進行了極大的簡化，同時還實現了自動化。



定期線上完成 PCI 自我問卷評估

PCI DSS 要求企業每 12 個月完成一次自我評估問卷 (SAQ) 的 QualysGuard PCI 支持基於 PCI DSS 要求的 SAQ V1.2。的 QualysGuard PCI 可使用戶快速，輕鬆地完成問卷，透過這個問卷充分了解目前 PCI 合規狀況。



保護 Web 應用程序以符合 PCI6.6 規範

現在 PCI6.6 要求必須確保 Web 應用程式的安全性。QualysGuard PCI 提供了一個自動化的工具來保護 Web 應用程式的安全，可用於開發前及開發後 web 應用程式的評估，以確保 Web 應用程式在開發及維護期間始終處於安全的狀態。

QualysGuard WAS 模組可讓用戶：

- 掃描 Web 應用程式（無論是企業內部自行開發或購買商業套裝軟體）均能檢測漏洞型態。
- 識別跨網站腳本攻擊 (Cross-site script) 之漏洞。
- 識別資料隱碼攻擊 (SQL Injection) 注入攻擊。
- 執行經驗證和未經驗證的掃描。



Qualys Secure Seal 安全標章

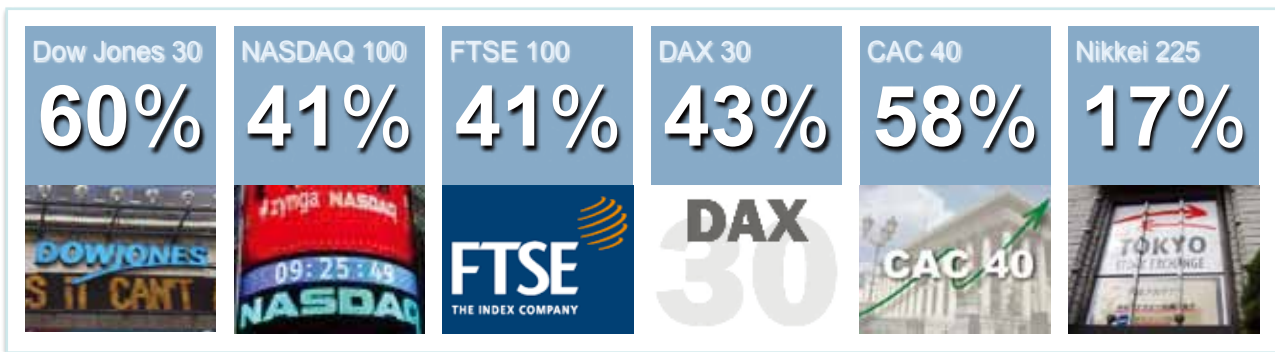
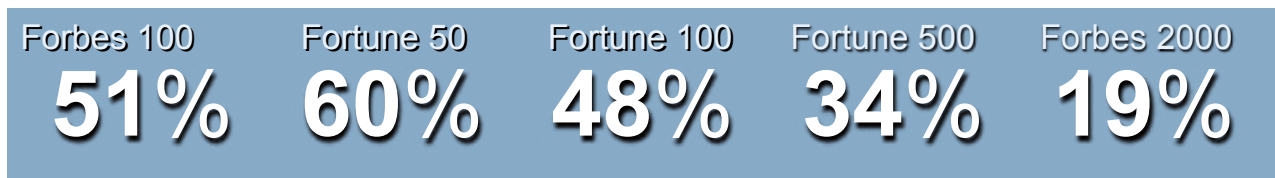
Qualys Secure Seal 安全標章，可以掃描企業網站是否存在惡意程式、Web 應用程式漏洞及 SSL 憑證驗證等功能，並可在您的網站使用 Qualys Secure Seal 安全標章，來對您的客戶展示，企業的網站已經過安全性檢測，已增進企業信譽形象。

Qualys 公司簡介

Qualys 成立於 1999 年並提出安全檢測及合規性方面提供量身訂做的解決方案，成功地完成弱點管理和政策合規方案。2000 年 12 月 Qualys 公司推出 QualysGuard，從此時起正式進入了漏洞管理這個新興的市場。QualysGuard 具備高度準確性及方便性之掃描技術，在弱點管理市場中，開創了透過網路即可進行弱點管理的革命性創舉。

Customers and Awards

根據富比士 (Forbes) 與財富雜誌 (Fortune) 的調查，全球前 100 大企業有近過半的企業均選擇 QualysGuard，因為 QualysGuard 是全方位弱點管理工具。



Qualys 為公認的領導品牌，

Qualys 在各個領域贏得無數的獎項，其中包括：

Gartner、Forst & Sullivan、SC Magazine 等，無疑地 Qualys 為最佳的弱點管理解決方案，所以我們深深相信此產品是您最佳的選擇！

