

# tenable.io™

## 針對現今的動態資產而建置的弱點管理

現今隨著威脅的增加及 IT 格局之不斷變化，識別弱點和威脅已讓資安團隊舉步維艱，而更重要的則是要修復這些弱點和威脅。隨著越來越多的組織採用雲端服務、行動裝置和 DevOps，資產之基本概念已發生變化，並且對資安團隊的工作方式造成影響。先前執行定期掃描的方法無法再提供管理現今動態資產所需的弱點可見性與洞察力。

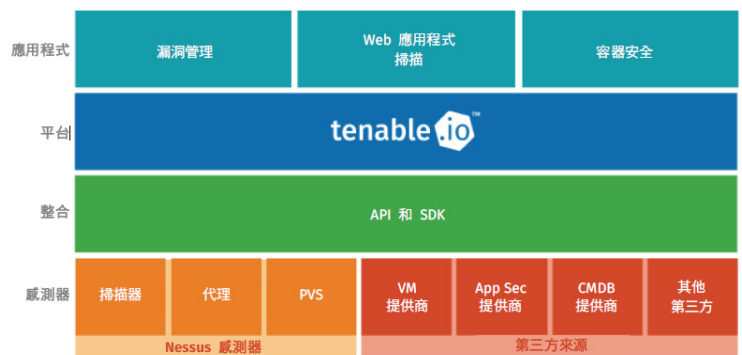
組織處理資產及其弱點的方法發生極大變化，在這種背景之下，由同一個管理平台匯集所有弱點資料（無論資料來源為何）比以往任何時候都更加重要。若僅能接受並管理個別的資料，此類解決方案實際上對管理者沒有幫助。考慮到組織解決資產和弱點的方法發生了上述變化，需要採用一種新型的方法來解決基本的弱點管理難題，並且不會對諸如採用雲端和 DevOps 等新科技的客戶造成不利影響。

## Tenable.io — 一個現代化弱點管理平台

Tenable.io 基於 Tenable 公司領先的 Nessus 技術建置，透過一種基於資產的新型方法，可以準確追蹤您的資源和弱點，展現您的安全及合規性狀態，同時調整雲端和 Container 等動態資產。Tenable.io 可提供最佳可見性和洞察力，並有效地對弱點設定優先順序，同時無縫整合至您的環境。

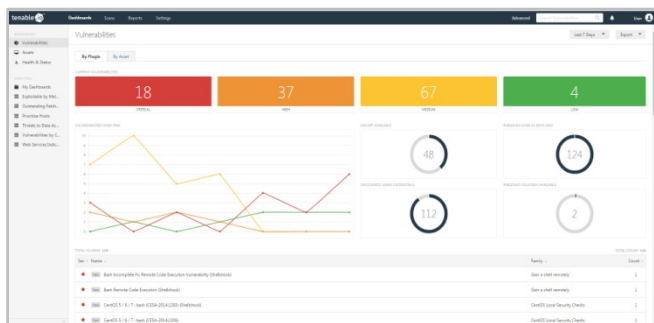
## 主要优势

- **消除盲點**：Tenable.io 為傳統及現代資產提供最全面的可見性，如雲端、行動裝置、Container 和 Web 應用程式等資產。
- **關注弱點狀態追蹤**：新發現的、活動中或重新出現的弱點，這些是您最關注的，Tenable.io 將這些內容顯示在前端及中心位置，以便您可以集中精力處理真正重要的事務。
- **透過優化使用者體驗提高工作效率**：利用最新且直覺的使用者介面以及應用程式裡所傳達的訊息，Tenable.io 有效引導您執行常見及複雜的工作。
- **透過各種簡化的整合方式達到最大化價值**：Tenable.io 已內建能互相整合的的系統，如特權帳號管理系統、修正檔管理系統和行動裝置管理 (MDM) 解決方案。
- **採用彈性資產授權模式提高投資回報率**：Tenable.io 採用一種基於資產的新型授權模式，每個資產僅會計算一個授權。



Tenable.io 應用程式能夠解決特定安全難題。這些應用程式共用同一平台，從而輕鬆在您的需求增長時新增能力。

該平台包括 Nessus 掃描引擎，使用 Agent 代理程式的主動式掃描和被動式流量監聽，也包括 API 和 SDK，這些都能在 Tenable.io 平台上建置並自動共用弱點資料。有越來越多的應用程式基於 Tenable.io 平台建置，解決現今最艱難的安全難題（包括弱點管理、Container 安全和 Web 應用程式掃描），從而方便管理者從一個應用程式開始使用，並在需求增加時再擴充其他應用程式。這種應用程式、資料感測器和自動化的組合提供風險最大覆蓋範圍，並對資產和弱點提供持續可見性 — 以便您可以採取更明智的行動來保護最重要的東西。



借助於直覺精簡的介面和多個內建儀表板和報告，Tenable.io 可輕鬆實現最高效率管理常用和複雜的工作。

## 主要功能

### 應用程式集中管理

Tenable.io 平台提供多個應用程式可明確的解決現今的安全挑戰，如弱點管理、Container 安全、Web 應用程式掃描以及即將加入的更多應用程式。這些應用程式基於共用平台建置，利用 Nessus 掃描引擎、API 和 SDK，並可以透過單一介面存取，進而便於啟動新應用程式並能夠立即轉變為生產力。

### 整合的 Container 安全

作為市場上唯一提供整合 Container 安全能力的弱點管理解決方案，Tenable.io 在 Container 建置前就考慮到了安全問題。這使得組織獲得對 Container 映像檔中所存在隱藏安全風險的可見性，並在上線使用之前進行補救，而不會延長改革週期。

### 最全面且價格實惠的掃描選項

Tenable.io 包含可以最大化掃描覆蓋範圍並減少弱點盲點的 Nessus 掃描引擎。掃描引擎同時包括主動式代理程式(Agent)掃描，以及被動式流量監聽 — 全部均無需額外付費。基於我們常用的 Nessus 技術，主動式掃描能夠對資產和弱點提供最廣泛的覆蓋範圍。使用代理程式的掃描和被動式流量監聽讓您能夠妥善管理暫時或遠端裝置等不易處理的資產，以及諸如醫療或工業控制裝置等敏感主機。

### 精準的資產追蹤

Tenable.io 能夠非常精確地追蹤資產及其弱點，從而為安全團隊提供最真實的環境視圖。該產品採用進階資產識別演算法，可準確指出您環境中每種資源的真實身分 — 甚至是諸如筆記型電腦、虛擬機器和雲端等動態資產。此演算法使用廣泛的屬性（如 Tenable ID、NetBIOS 名稱、MAC 位址等）來準確追蹤資產變化，而不論它們的漫遊方式或持續時間為何。

### 提供 API 使用文件 和 整合的 SDK

輕鬆自動化 Tenable.io 能力和弱點資料的共用，或基於 Tenable.io 平台建置，進而利用完整的 API 和 SDK。使用這些工具能最大化弱點資料的價值，無需增加額外成本。

### 保證正常執行時間的 SLA

Tenable 透過 Tenable.io 穩健的服務等級協定 (SLA) 提供弱點管理業的第一個正常執行時間保證。如果未達到 SLA 則提供賠償金，如同 Amazon Web Services 這類領先的雲端提供商一樣。

## 培訓

Tenable 為 Tenable.io 的新使用者以及希望瞭解在最大程度上利用該產品之知識及技能的使用者提供培訓，並為經驗豐富的使用者提供進階主題。

課程透過 Tenable 網站按需提供。



更多資訊：請瀏覽 [tenable.com](https://tenable.com)  
與我們連絡：請傳送電子郵件至 [sales@tenable.com](mailto:sales@tenable.com) 或瀏覽 [tenable.com/contact](https://tenable.com/contact)

版權所有 © 2017。Tenable Network Security, Inc. 所有權利均予保留。Tenable Network Security 和 Nessus 是 Tenable Network Security, Inc. 的註冊商標。Tenable 和 Tenable.io 是 Tenable Network Security, Inc. 的商標。其他所有產品或服務均為各自所有者的商標。ZH-TW-01312017-V11