

# NESSUS EXPERT

## 專為現代攻擊破綻而 打造

今日我們對攻擊破綻的看法大大有別於 1998 年 Nessus 剛問世時。資安從業人員現今的難題在於無法面面俱到地保護企業，而威脅執行者卻能游刃有餘地利用無數的弱點和漏洞發動攻擊。

資安從業人員、顧問、開發人員和滲透測試人員需要弱點評估解決方案來應對會使日益擴大的攻擊破綻倍受影響的威脅。新的攻擊媒介以超乎傳統 IT 資產意料的方式冒出，例如面向外部的雲端基礎架構和各式資產，而企業卻毫不知情。

## 加強企業的評估工具組

Nessus 是業界最受肯定的弱點掃描器，而 Nessus Expert 則建構在此傳奇之上，成為市面上第一套可提供整個現代攻擊破綻能見度的弱點評估解決方案。Nessus Expert 擴充了 Nessus Professional 的功能，透過為企業提供基礎架構即程式碼 (IaC) 部署評估並搜尋曝露在網際網路上的資產，洞悉傳統 IT 資產以外的風險，採用統一集中管理。

## 涵蓋範圍的廣度與深度

Tenable Research 與資安社群密切合作，不斷搜尋新弱點，並提供分析洞見，協助企業執行更健全的弱點評估做法。Tenable 的零時差團隊在過去 3 年中發現了 100 多個零時差弱點。

## NESSUS 在弱點評估 領域排名第一

### 準確度領先

Nessus 擁有業界最低的誤報率，準確度達到六個標準差（每一百萬次掃描中僅有 0.32 次誤報）。

### 涵蓋範圍領先

Nessus 能提供最深入、最廣泛的涵蓋範圍，CVE 數量多達 62,000 多個，並且每週在弱點披露 24 小時內即發佈 100 多個最新 plug-in。

### 採用率領先

Nessus 受到全球 30,000 家以上的企業信任，下載次數達 200 萬次。有半數的財星 500 大企業以及 30% 以上的全球 2,000 大企業都仰賴 Nessus 技術。

搜尋及評估企業的  
IT 資產

+

在部署前保護雲端基礎架構  
的安全

+

掌握網路連線的攻擊破綻  
能見度

# 提早執行與保障雲端基礎架構

隨著雲端服務和基礎架構的興起，部署新應用程式和工作負載可能並不難。但快速敏捷的部署方式會在這些環境中衍生更多未知的網路風險。現在，市面上已經有專為保護雲端而設計的解決方案，但是應用時卻緩不濟急。使用 Nessus Expert 可讓企業將程式推送至生產環境前掃描 IaC 程式碼存放庫，以防止未知風險。

## 關鍵優勢：

- 制定主動評估雲端工作負載弱點的方式。
- 在軟體開發生命週期 (SDLC) 中找出未知的安全問題。
- 在部署程式碼之前找出會中斷營運且代價高昂的弱點。

# 掌握網際網路連線的攻擊破綻能見度

現代攻擊破綻是因面向網際網路的資產所致，企業往往不清楚這些資產的現況，除了無法控管資產庫外，開發人員能夠在幾分鐘內開啟若干雲端執行個體，使這些執行個體來去如風。從攻擊者的角度來看，透過面向網際網路的資產可以輕鬆卻隱密地刺探弱點與滲透網路，尤其是在當您並不知道這些資產曝露在誰面前或甚至不清楚這些資產是否存在的情況下。使用 Nessus Expert 可搜尋及評估這些未知資產。

## 關鍵優勢：

- 可搜尋企業過去並不知道的網際網路連線資產
- 開始對新找出的資產進行評估掃描
- 瞭解企業邊界外的資產風險並消弭落差

## 善用 PREDICTIVE PRIORITIZATION 的強大功能

利用 Tenable 的弱點優先順序評分 (VPR) 協助企業查明其環境中造成最大風險的特定弱點。VPR 將 Tenable 收集得來的弱點資料與第三方弱點及威脅資料結合，並利用 Tenable Research 開發的先進資料科學演算法一併加以分析。

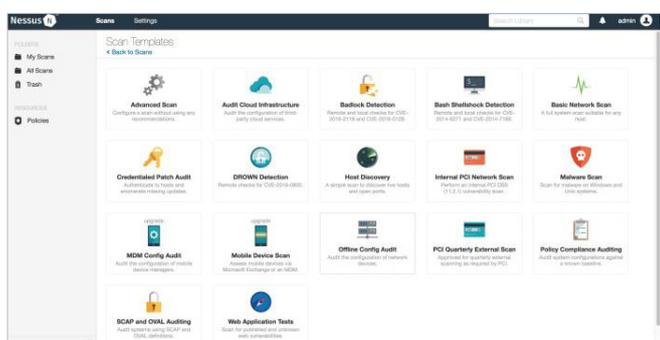
# 簡單易用

Nessus 是由資安從業人員專為資安從業人員所打造，其核心宗旨就在於為奮戰在第一線的資安專業人士帶來直覺式的使用體驗，以便更快速、更充滿信心地發現並修復弱點。

使用者介面更新讓導覽和使用者體驗變得更輕鬆、更符合直覺。Nessus 最新的資源中心可為使用者提供隨手可得的相關資訊。使用者專用指南載有操作方式與執行功能的可行秘訣和指引。

## 透過預先建立的原則和範本快速發現弱點

適用於 IT 和行動資產立即可用、預先設定的範本，提供高效的設定稽核，協助您快速找到弱點所在之處。



450 多個合規性和設定範本，以便您根據 CIS 標準和其他最佳做法來稽核設定和合規性。

## 「即時結果」的智慧弱點評估功能

「即時結果」能夠在離線模式下以最新 plug-in 執行智慧弱點評估，您無需再執行掃描。只需登入並在掃描歷史記錄中查看潛在弱點的偵測結果即可。按下按鈕，您就可以執行掃描以驗證是否存在弱點，建立更高效的問題評估、排定優先順序與修復流程。

## 輕鬆自訂報告

根據自訂的分析方向(如特定弱點類型、按主機/plug-in、團隊/客戶分類弱點)輕鬆建立報告，支援多種格式(HTML、CSV 和 Nessus XML)。

## 深入瞭解和疑難排解

當網路變得愈趨先進複雜，要查明可能發生的問題也會變得越來越耗時。Nessus 封包擷取功能可提供解決客戶掃描問題的強大疑難排解能力。

## 利用群組式檢視提供專注力

類似的問題或弱點類別會被歸類在一起，並呈現在單一串列中。靜音功能可讓您選擇哪些問題在指定的期間內不要顯示在檢視畫面中。這有助於排定問題的優先順序，讓您在既定時間內更加專注於解決當務之急。

## 可攜且彈性

為了可攜性和使用方便，Nessus 現已可在 Raspberry Pi 上使用。這個特性對於滲透測試人員、顧問和需要在不同地點之間頻繁往返的工作人員而言特別實用。

# 提供進階技術支援

只要訂閱進階等級的技術支援，Nessus Professional 客戶即可 365 天全年無休 24 小時全天候使用電子郵件、入口網站、對談及電話支援。這也有助於確保加快回應時間及解決問題的速度。支援方案相關完整詳情載於[此處](#)。

# 關於 TENABLE

Tenable®, Inc. 是一家 Cyber Exposure 分析公司。全球超過有 30,000 家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了自己在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含超過 50% 的財星 500 大企業、超過 30% 的全球 2,000 大企業以及大型政府機構。如需深入瞭解，請前往 [zh-tw.tenable.com](http://zh-tw.tenable.com)。

如需詳細資訊：請前往 [zh-tw.tenable.com](http://zh-tw.tenable.com)  
與我們聯絡：請寄電子郵件至 [sales@tenable.com](mailto:sales@tenable.com)  
或前往 [zh-tw.tenable.com/contact](http://zh-tw.tenable.com/contact)