tenable Security Center Plus

產品說明

善用內部部署的風險型弱點管理方法 提升安全方案的成效

洞察一切、預測最重要的事、內部管理，Tenable Security Center Plus 幫您實現。

> 「這是一套全方位的 Tenable 解決方案，讓我能隨時根據業務目標排定安全風險的優先順序，並評估企業的安全狀況。」
>
> - 某醫療服務供應商

隨著 IT 技術的不斷變化和網路威脅的不斷演進，定期掃描和合規性稽核對於企業抵抗新型網路攻擊的效果已大不如前。為確保企業的安全，您需要一套完善的弱點管理解決方案，讓您可以全面掌握攻擊破綻，以便有效管理和衡量您的網路風險。

以 Nessus 領先技術為基礎的 Tenable Security Center Plus 是市場首屈一指的弱點管理平台，可提供新一代的弱點管理內部部署方案。透過先進的分析工具，可自訂功能的儀表板、報告與工作流程，Tenable Security Center Plus 可協助企業掌握弱點管理的要領並降低企業風險。

運用 Predictive Prioritization 結合涵蓋多個來源的資料與威脅情報，藉此預測弱點遭到攻擊的可能性，並與企業動態資產在瞬息萬變環境中的重要性相匹配。成果就是企業得以檢視弱點及與弱點有關的最重要資產，並排定優先順序，讓企業據此安排可行方案，保障企業安全，預防影響業務營運的資料外洩。

圖 1：可高度自訂的儀表板、報告、工作流程和安全原則，滿足特定業務需求。

Tenable Security Center Plus 包含超過 350 個可高度自訂的內建儀表板和報告，有助於迅速瞭解安全合規性、成效和風險。您可以根據管理階層所關心的高階業務目標和可自訂的基本原則持續衡量、分析及查看安全方案的成效。

關鍵優勢

- **不中斷的能見度**

  持續不斷地追蹤已知並搜尋未知的資產及其弱點。察覺威脅及非預期的網路變更，在演變成弱點前防患於未然。

- **被動式弱點偵測**

  針對資產進行的被動式弱點偵測不僅可執行準確的時點掃描，還能搜尋記錄檔並進行深入分析以偵測出資產的變更，最終消除盲點。

- **排定資產與弱點的優先順序**

  將資產和弱點資料、威脅情報與資料科學加以整合，估算出淺顯易懂的風險評分，以便快速找出弱點以及與該弱點相關、會對企業造成最大風險的最重要資產。

- **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 可察覺 79,000 多個弱點，擁有業界最廣泛的 CVE 和安全組態支援能力，協助您瞭解所有的曝險。

- **自動化處理流程**

  充分運用詳實記錄的 API 以及預先建置的整合功能來匯入第三方資料、自動化掃描並與 IT 系統共享資料。

關鍵功能

讓企業自行選擇管理資料的方式

Tenable Security Center Plus 是市場首屈一指的弱點管理內部部署方案。利用內部部署或配合企業最繁複部署需求的多元部署方案，在降低貴公司風險的同時，讓企業自行選擇管理資料的方式。

完備的評估選項

Tenable Security Center Plus 能為企業提供整個攻擊破綻的統一能見度。它充分運用 Nessus 感應器(包含主動掃描器、代理程式、被動式網路監控和 CMDB 整合功能)，能協助涵蓋最多的基礎架構掃描範圍並減少弱點盲點。多元的資料感應器類型有助於企業同時追蹤及評估已知和未知的資產及其弱點。

被動式弱點偵測

針對資產進行的被動式弱點偵測不僅可執行準確的時點掃描，還能搜尋記錄檔並進行深入分析以偵測出資產的變更，最終消除盲點。

根據實際風險排定弱點的優先順序

Tenable Security Center Plus 將弱點資料、威脅情報與資料科學加以結合，估算出淺顯易懂的風險評分，以便企業排定弱點的優先順序並知道哪些弱點應該優先修復。您可快速評估風險並找出對貴公司影響最大的弱點。

簡化弱點管理

透過直覺化的報告和一目瞭然的儀表板以及簡便好用的介面，Tenable Security Center Plus 能讓常見任務(如設定掃描、執行評估與分析結果等)比以往更輕鬆。預先定義的掃描範本、設定與合規性稽核檢查皆遵循最佳做法框架，讓企業只需要花費跟之前相較九牛一毛的心力，即能獲得保障。使用預先設定、立即可用的儀表板來自訂報告與分析，亦可快速地從頭建立符合企業需求的專屬報告與分析功能。

瞭解資產重要性

運用 Tenable 透過 Tenable Security Center Plus 提供的 Asset Criticality Rating (ACR)，根據業務價值與重要性指標來預測資產的優先順序。Asset Criticality 搭配 Predictive Prioritization 可相輔相成，組成最符合企業需求的弱點管理方法，使企業知道首要之務是哪些弱點及其相關資產。

Tenable One 整合功能

輕鬆將 Tenable Security Center 資料與 Tenable One 整合在一起，開始邁向曝險管理的旅程。充分利用 Lumin Exposure View、Attack Path Analysis 和 Asset Inventory 等先進功能的優勢，取得現代攻擊破綻的統一能見度並主動管理網路風險。

簡化合規性

透過預先定義的檢查、指標並在違反產業標準和法規規範時發出主動警示等功能，使企業洞察並通報合規性。產業標準包括 CERT、NIST、DISA STIG、DHS CDM、 FISMA、PCI DSS、HIPAA/HITECH 以及其他多項標準。

內部部署的 Web App Scanning

透過內部部署的 Tenable Web App Scanning，輕鬆整合 Tenable Security Center 資料。在 Tenable Security Center 使用者介面中設定新的掃描並分析 Web 應用程式曝險。Tenable Web App Scanning 能夠為新型 Web 應用程式進行自動化全面弱點掃描，功能簡便好用，不需耗費大量人力，企業便可以快速評估 Web 應用程式。

Tenable Research

Tenable Security Center Plus 以 Tenable Research 作為後盾，提供世界級的網路曝險情報、資料科學見解、警示與安全公告。Tenable Research 頻繁更新的內容，可確保提供即時的弱點檢查、零時差研究與組態指標，有助於保障貴公司的安全。

善用 Tenable Security Center Director

Tenable Security Center Director 是一項提供集中式管理及檢視企業風險態勢的附加元件，它能跨整個企業部署使用的多個主控台，掌握全盤的能見度。

預先建立的整合功能與詳實記錄的 API 及整合式 SDK

Tenable 弱點管理具有經認證的掃描、SIEM、SOAR、工單與修補系統以及其他輔助解決方案等立即可用的整合功能，企業得以輕鬆簡化弱點管理流程。完整清單請見此處。另外，您也可以使用詳實記錄的 API，在 Tenable Security Center Plus 中輕鬆地自行建立整合功能。使用這些工具無需額外成本，就能發揮相關弱點管理使用案例的最高價值。

如需詳細資訊：請寄電子郵件至 sales@tenable.com 或前往 zh-tw.tenable.com/contact