VMware Aria Automation for Secure Hosts

主要優勢

- 強制落實安全性 - 運用強大的自動化弱點修復功能，針對地端或雲端基礎架構的重大安全性威脅進行補救。
- 維持合規性 - 使用內容經過認證的現成 Center for Internet Security (CIS) 管理指南，從一開始佈建 IT 系統時就符合標準，並維持合規。
- 降低風險 - 利用強大的安全主機自動化功能，不僅能掃描重大 IT 弱點及合規問題，更能找出缺失並進行修正。

VMware Aria Automation™ for Secure Hosts 是 VMware Aria Automation 的合規與弱點管理附加元件，針對 IT 系統合規及弱點修復提供完善服務以及封閉式迴圈自動化。透過 VMware Aria Automation for Secure Hosts，資安團隊和營運團隊即可在單一平台上協同合作，依據企業 IT 安全性原則進行系統掃描、弱點偵測和找出未合規的問題，並主動進行修復。

圖 1：VMware Aria Automation for Secure Hosts 為 VMware Aria Automation 增加基礎架構安全性和合規

專為現代化安全性需求所打造

資安團隊和 IT 營運團隊必須合作來確保現代資料中心符合標準且安全無虞，但往往由於採用不同的工具組、不一致的工作流程和相互衝突的優先順序，導致事倍功半。VMware Aria Automation for Secure Hosts 是強大的 VMware Aria Automation 附加元件，為 IT 營運團隊和資安團隊提供所需的自動化工具和內容，以打造和維護安全且符合標準的地端或雲端 IT 基礎架構。VMware Aria Automation for Secure Hosts 可提供持續的作業系統合規施行、自動化弱點偵測和修復，以及 IT 系統狀態的即時洞悉。

若要取得更多資訊或購買 VMware 產品

請致電 +886-2-3725-7000、造訪 vmware.com/tw/products 或線上搜尋授權經銷商。如需詳細的產品規格和系統需求，請參閱 VMware Aria Automation for Secure Hosts 說明文件。

預建認證 IT 安全性內容

大部分企業都必須遵循多種法規和標準，每種又各有數千項個別要求和檢查。VMware Aria Automation for Secure Hosts 包含的資料庫，以 CIS 和美國國防通訊局安全技術實作指南 (DISA STIG) 架構為基礎，囊括最新的受認證安全性內容，團隊只要執行一個動作即可偵測合規問題，同時強制執行多種合規標準的要求。

持續落實合規

追蹤現有系統的合規變動，是管理者日覆一日的夢魘。VMware Aria Automation for Secure Hosts 會主動掃描合規變動並提供自動化修正的指導手冊，依照企業安全性原則強制執行，進而節省資源、改善安全態勢並降低風險。

VMware Aria Automation for Secure Hosts 可實現協同作業和快速執行治理和控制。管理員能套用角色型存取控制，讓資安和 IT 專業人員在職責範圍內定義合規與安全性原則，並根據原則掃描系統、修正問題及追蹤趨勢。

持續不中斷的弱點管理

安全性掃描工具可能會回報大量弱點，營運團隊必須將這些弱點轉換成 IT 支援工單，加以調查、排定優先順序、測試、修正，然後再回報給資安團隊。VMware Aria Automation for Secure Hosts 為營運團隊提供弱點自動化的強大功能，針對超過 15,000 項作業系統和基礎架構弱點掃描 IT 系統，並提供現成可用的自動化弱點修復工作流程。

除了原生弱點掃描功能，VMware Aria Automation for Secure Hosts 還能匯入 Tenable、Rapid7、Qualys 及 Kenna 等第三方解決方案的掃描結果，並迅速執行自動化弱點修復。

圖 2：追蹤 IT 弱點，運用現成可用的自動化工作流程進行弱點修復

文件編號：1861500aq-ds-vmw-aria-auto-sec-hosts-A4_TW