HCL SOFTWARE | BIGFIX

HCL

選擇端點合規解決方案以改善您的安全狀況

IT 營運和安全團隊的解決方案指南

面對日益出現的安全攻擊，建立和維護一個由不同的軟硬體與網路組件組成的安全 IT 環境，給當今很多組織帶來了嚴峻的挑戰。 許多 IT 營運和安全團隊不斷地尋求更有效的方法來增強安全狀態，並在對抗入侵的同時，降低成本和複雜性與提高生產力。

合規是一個概念，起源於證明組織有能力遵守幫助組織更加安全的要求、規則或政策。當組織遵守特定產業的安全法規（如：PCI DSS、HIPAA）和通用安全準則（如：ISO 2700x）時，則可避免了許多安全事件。

本解決方案指南，著重於介紹組織在選擇有效的端點合規解決方案時應考慮的問題，來改善組織的安全狀態並成功實施合規計劃。

什麼是 IT 合規？

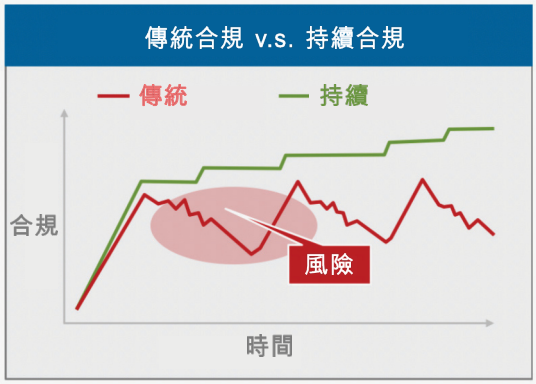
IT 合規包含組織在所有涉及 IT 實體活動（包括人、機器、網路、流程和過程）中定義和執行的一套政策或規則，以提供更高級的監管或商業政策，保護 IT 基礎架構不受惡意活動的破壞。端點管理的合規是一套與端點相關的政策，這些政策被定義、執行與監控，以幫助組織有效地管理和保護其端點。端點管理的合規是 IT 營運和安全團隊的基本職責。

組織要實行端點合規，需要具備以下四種基本能力：

1. **策略制定：**定義並實行政策，以滿足法規或公司的具體要求。
2. **端點評估：**根據策略評估每個端點的狀態（系統配置、註冊表、屬性等）。
3. **分析與報告：** 收集、匯總和分析評估結果，並根據政策報告合規狀態。
4. **不合規的補救：**對不合規的端點採取補救措施，以執行政策。

理想的情況是，所有四種功能都可由一個有效的端點合規解決方案提供。無論其位置和網路連接如何，該解決方案都可以解決各種端點類型和操作系統的問題。

雖然合規性的目標是降低安全風險，但許多組織沒有認知到，如果合規解決方案不能持續地提供合規，那麼它可能無法有效降低風險。傳統的合規方法是定期評估端點和補救不合規，當合規水平在定期合規週期之間的時間間隔內下降時，就會出現安全風險增加的缺口。相比之下，持續合規方法則是不斷監測端點並糾正不合規行為，從而使合規水平保持在較高的水平，消泯風險缺口。



持續合規降低風險

三項關鍵端點合規活動

端點合規應該解決以下三個活動，以有效保護端點的安全：

1. **修補程式和漏洞管理**：安裝在端點上的作業系統和應用程式應該應用哪些修補程式？在漏洞被惡意軟體利用之前，應該多快應用這些修補程式？
2. **安全配置管理**：如何正確設置和維護作業系統和應用程式的安全相關配置，以防止端點因配置錯誤而被入侵？
3. **端點防護工具管理**：應該部署哪些端點保護工具來保護端點不被攻擊？如何確保工具始終正確部署和運行？

修補與漏洞管理

根據美國國家標準與技術研究所的定義，漏洞是指軟體（作業系統或應用程式）中存在的弱點，一旦被利用，就會對保密性、完整性或有效性產生負面影響。雖然存在多種類型的漏洞，但最主要的類型是導致黑客通過"後門"獲得端點上的特殊權限，並植入和執行惡意程式碼，以竊取儲存在端點上的寶貴資訊或使端點無法正常使用（如：勒索軟體）。正如許多安全研究人員所報告的那樣，軟體漏洞仍然是外部入侵導致安全漏洞的主要原因。迅速識別和修復漏洞是許多組織的 IT 安全和營運團隊的首要任務。

儘管許多軟體供應商已經採用實施安全工程，如：滲透測試和應用程式掃描，但軟體漏洞仍持續地激增。針對所有作業系統和應用漏洞的最佳保護措施是不斷地修補一切漏洞，但這說起來容易做起來難。

定義一個合規性政策可能很簡單，例如："在修補程式可用後30天內，將所有嚴重程度較高或關鍵的安全修補程式應用到所有伺服器上"。執行這一政策的實際做法可能會很複雜，因為它需要考慮多種因素，如：對正常日常營運的影響（有些修補程式需要重新啟動端點）、根據一群伺服器之間的關係（如：Web伺服器、應用伺服器和資料庫伺服器）而產生的修補順序，以及與應用程式的向下相容。

安全配置管理

由硬體供應商提供的帶有作業系統和一些預裝應用程式的電腦通常沒有進行安全配置。這些不安全的配置可能包括，但不限於：

- 未正確設置目錄和檔案權限
- 沒有默認或非常弱的密碼策略（密碼強度、年齡、歷史記錄等）
- 沒有記錄所有的管理或用戶帳戶/登入活動
- 有些服務默認不被停用。
- 默認允許遠程訪問
- 主機防火牆允許主動連接
- 默認情況下不啟用儲存加密（如果可用）。

不安全的配置是入侵或網路攻擊的另一個主要原因。國家漏洞資料庫中報告的許多漏洞都與不安全的配置有關，需要透過更新配置設定而不是使用修補程式來解決。

因認知到安全配置對於建立安全的電腦環境和防止入侵至關重要。一些權威組織已經發布了安全指南或基準，如：網路安全中心（CIS）基準、國防資訊系統局安全技術實施指南（DISA STIGs）、支付卡行業數據安全標準（PCI DSS）。這些指南為組織提供了建立以安全配置為重點的合規政策的最佳典範實務。由於入侵技術不斷發展，這些指南也在不斷演進，以提供合宜的保護，這也意味著組織需要不斷更新其安全配置合規政策，以採用最新的最佳典範實務。

端點保護工具管理

修補程式和維護安全配置應被視為端點安全的基本 "保健"。然而，端點仍然需要使用各種端點保護工具，如：防毒軟體、防惡意程式軟體、端點檢測和回應（EDR）、應用程式控制、數據遺失預防、加密、網路過濾和安全電子郵件等來保護端點免受網路攻擊。

從合規政策的角度來看，端點保護工具必須適當部署在目標端點上，並保持運行以提供預期的保護。如果一個工具停止運行或不是最新的(例如，防病毒軟件在運行時病毒定義已經過時)，就需要盡快檢測和補救。

端點合規成熟度模型

目前市場上存在多種端點合規解決方案，通常是作為供應商端點管理或安全套件的一部分。然而，並非所有的解決方案都能提供所有四種基本功能或解決前面所述的三種合規活動。因此，可對保護組織端點的端點合規解決方案之成熟度進行分析和分類。

評估端點合規解決方案能力的成熟度模型

	初級	執行級	優化級
策略制定	工具可用，但沒有開箱即可用的實用內容來幫助制定策略	有限的策略內容，或需要將內容轉化成機器可執行的腳本或檢查清單	策略內容豐富，其基於產業指南或和基準且開箱即用，也容易部署易於客製化
端點評估	僅在預設時間或按照需求啟動遠端掃描	在預設時間掃描，兩次掃描之間沒有評估	持續評估，可立即發現配置偏移與策略衝突，無須掃描
分析與報告	僅根據上次一次性掃描結果，來更新最新狀況	根據多次累積的掃描結果，來更新最新狀況	根據企業與定義群組間持續地評估結果，來更新最新狀況與歷史趨勢
不合規的補救	無須補救，需要單獨採取臨時方法	提供修復功能，但需要手動回應	無須人工干涉，可自動修復不合規端點，消除漏洞缺口

- **初級：**初始水平的解決方案只包含四種基本能力的一部分。即使是支援的功能，該解決方案也可能需要額外的人工作業或其它工具來實現所需的合規水平。例如：可能沒有開箱即用的策略內容來幫助組織快速創建合規策略，或者只能從伺服器遠端啟動端點評估。

- **執行級：**執行達到成熟的解決方案可以提供所有四種功能，但有一些限制，無法實現最佳的端點保護，或需要額外的人工作業。例如：對於策略建立，解決方案提供的內容有限，因此可能需要額外的開發來實施所需的策略。在某些情況下，這些內容是以一種需要在部署前轉換為機器可執行腳本的格式提供的。此外，該解決方案可能會定期掃描端點，但在掃描之間沒有進行合規狀態評估，允許配置偏移或違反策略，從而為網路攻擊創造了一個大的風險破口。該解決方案可能提供分析和報告，但該解決方案可能只根據每次掃描結果來描述狀態。補救措施可能是解決方案本身提供的，但只能手動執行--延長了修復策略違規和漏洞破口的時間。

- **優化級：**優化達到成熟度的解決方案以非常有效和自動化的方式提供所有四種功能，使企業能夠優化其保護端點安全和實現合規的做法。該解決方案根據 CIS 和 DISA STIG 等行業最佳實踐基準，提供豐富的開箱即用的策略內容，而且這些內容可以立即使用並易於自訂。優化的解決方案可以對端點進行持續評估，以即時發現配置偏移或策略違規。持續評估的方法是改善組織安全狀態、降低網路攻擊風險破口的最有效方法。

優化後的解決方案還可以分析和報告當前狀態和歷史趨勢，以全面了解整個組織、一組端點（如：在 Windows 上運行的所有端點）或單個端點的安全狀態。使用優化的解決方案，可以在沒有任何用戶干預的情況下自動糾正不合規行為，從而大大減少漏洞破口。

組織很可能會發現，目前市場上的大多數端點合規性解決方案可分為"初級"或"執行級"成熟度級別，很少有解決方案在"優化級"成熟度級別上提供所有四種功能。

透過 BigFix 合規來優化安全合規

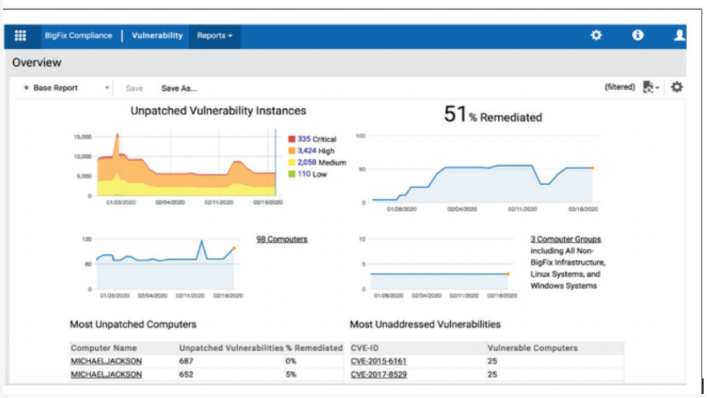
BigFix 合規是 HCL 的 BigFix 端點管理組合中的解決方案，可確保組織所有端點持續遵守安全和監管政策。它是目前市場上最先進的端點合規性解決方案之一，其提供所有四種合規功能並覆蓋所有三種合規活動，達到了 "優化級 "的成熟度水平。 BigFix 合規的特點包括：

- **豐富的檢查清單：**包含超過 20,000 項開箱即用的檢查，適用於 Windows、macOS、Linux 和 UNIX 的 60 多個作業系統、中介軟體和應用程式（資料庫、Web 伺服器、Web 瀏覽器）。這些檢查列表基於安全基準，包括：CIS、DISA STIG、USGCB 和 PCI DSS。這些檢查大大減少了創建策略的工作，並減少了為滿足多種監管和業務要求所需的開發工作。其也可以隨時部署並且易於自訂。 BigFix 團隊會不斷地更新檢查列表，以增加對最新基準檢查的支援，為駭客採用的新入侵或網路攻擊技術提供最佳保護。

- **持續評估：**由 BigFix 智慧代理根據部署的策略對每個端點的狀態進行持續評估。每個端點的合規狀態都會被持續收集，並立即反映在 BigFix 管理控制台中。持續的合規性監控被認為是檢測配置偏移和策略違規的最有效方法。BigFix 支援的所有作業系統和應用程式都採用相同的方法，因此組織無需採用多種解決方案來滿足不同平台的合規需求。

- **全面的合規分析和報告：**使用 BigFix 合規，所有端點的合規狀態都會被持續收集與匯總，並使用開箱即用的合規報告來描述整個端點環境、一組端點或單個端點的當前狀態和歷史趨勢，使安全和 IT 營運團隊能夠評估整體安全狀態，追蹤一段時間的合規，並快速識別需要採取行動的安全風險。

合規漏洞報告



- **內建自動修復功能：**一旦檢測到配置偏移，BigFix 的智慧代理可以立即將其恢復到所需的設置，而無需任何用戶干預。在這方面，BigFix 代理實現了端點的 "自我修復"。 BigFix 合規還提供了將嚴重不合規的端點與網路隔離的功能，以防止零日漏洞攻擊，直到完成適當的修復。

- **端點保護工具管理**：BigFix 合規包含一個端點保護的客戶端管理模組，用於監控和管理微軟(Microsoft)、賽門鐵克(Symantec)、McAfee、趨勢科技(Trend Micro)和 Sophos 等各種防病毒工具的部署狀態和運行狀況。除了報告整體的防毒部署運行狀況外，它還提供補救行動，以快速解決策略不合規問題，如：防毒代理未運行或病毒定義過時。

- **修補程式管理**：迅速達到首次成功率 98% 以上的修補程式管理，減少了漏洞的破口。 BigFi x合規中包含的 BigFix 修補程式支援 Windows、Linux、UNIX 和 macOS 作業系統以及 VMWare ESXiTM 管理程式。最重要的是，當修補程式下載到本地端的 BigFix 企業伺服器時，會自動評估所有端點，以確定適用性或相關性。

- **與其它行業領先解決方案的整合**：與其它行業領先解決方案的整合　可實現更深入的端點智慧、更好的風險檢測和更快的漏洞修復。可用的整合包括 IBM QRadar、Carbon Black EDR 和 Forescout 網路訪問控制（NAC）。

總結

建立和維護一個安全的 IT 環境，以應對日益增長的網路攻擊，仍然是 IT 營運和安全團隊面臨的巨大挑戰。組織應該實施 BigFix 合規這樣的合規解決方案，優化所有關鍵的端點合規活動，並管理安全策略的整個生命週期。 BigFix 合規為那些希望施行最佳典範實務以改善組織端點安全狀態，同時向內部利益相關者和外部監管機構展示合規的組織提供了巨大價值。 BigFix 合規還憑藉其獨特的能力，提供持續和自動的端點評估、分析和修復，縮小漏洞和網路攻擊的風險破口，同時顯著地降低實施有效合規計劃的複雜性和成本，從而與其他合規解決方案區分開來。

欲了解更多資訊或安排演示，請瀏覽 BigFix.com 或聯繫您的 BigFix 銷售專家。

HCL軟件是HCL科技公司（HCL）的一個部門，包含敏捷開發、DevSecOps、任務自動化、協同工作、資料管理、數位化行銷和電子商務以及主機軟件等領域的20多個產品系列，為客戶提供從雲交付框架，資料庫，應用服務，開發工具到移動使用的端到端的能力。
HCL軟件在世界各地設有辦事處和實驗室，為成千上萬的客戶提供服務。我們的使命是通過對產品的不懈創新，推動客戶的IT投資獲得最終的成功。

瞭解更多：https://www.hcltechsw.com

版權所有 © 2020 HCL Technologies Limited