BIGFIX
High Performance Security & Systems Management

在企業範圍內實現持續性的端點安全設定遵循

超越遵循，實現主動的設定管理
即時評估，調解及修復

除了防範日益增長的隱匿安全威脅，企業需要獲取越來越詳細的關於系統及安全策略的資料以證明其 IT 管理遵循相應的監管標準。許多組織經歷過失敗的安全審核，這些失敗的審核暴露出來的問題通常包括 1) 系統設定漏洞的能見度極差，2) 管理不佳或設定錯誤的系統。這些使企業去尋求設定管理解決方案，但現有的解決方案存在許多問題：手工的審核方法、報告及修復過程異常複雜和昂貴、漫長和痛苦的設定處理及修復週期、過多不可整合的單一功能產品帶來衆多異類的、互不關聯的資料等等。

BigFix 安全設定管理 (SCM) 為 IT 策略和標準遵循過程帶來了可驗證的即時可見性，自動化的設定修復和全球規模的可擴展能力。BigFix 的 SCM 是全面的技術控制項庫，可使用業界的最佳實踐和標準來檢查和執行安全設定策略，幫助組織達成 IT 安全遵循。SCM的策略庫能使遵循解決方案的快速執行符合每個用戶的需求。

產品收益

在全球數百萬台工作站，伺服器和行動設備上持續地執行安全設定基準 - 全部採用單一控制點

- 利用標準化組織提供的安全專業知識和指導，使用基於遵循性的設定檢查列表安全地設定系統
- 即時報告，修復任何偏離遵循標準的資產並確認修復結果
- 不管電腦的位置、OS、連結狀態或安裝的應用程式,都可獲得關於其健康狀態和安全性的有意義的資訊，並在企業範圍執行最優的使用策略
- 強化並統一遵循生命週期；將端點設定和修復時間由數天和數周減少到數分鐘和數小時

產品特點

- 全面、即時的管理視野可覆蓋所有電腦 - 即使是遠端和行動的端點
- 單一的集中化控制臺視圖可即時查看所有端點的當前設定狀態
- 簡單易用的遵循性展示板具備靈活的特殊查詢和彙報能力
- 易於部署的檢查列表包含數百種標準設定設置，可對應衆多業界的標準和規範，如美國國防資訊系統局 (DISA) 規範和安全技術實施指南 (STIG)，美國聯邦桌面核心設定 (FDCC) 等，除此之外，用戶還可根據需要整合和修改相應的設置
- 通過持續性的驗證設定變更的執行和修復通過自定義展示板即時監控設定遵循性

BIGFIX
High Performance Security & Systems Management

在企業範圍內實現持續性的終端安全設定遵循

系統及伺服器需求

BigFix 伺服器支援的作業系統

Windows 2003 Server

BigFix 伺服器的資料庫需求

SQL Server 2005

BigFix 控制臺支援的作業系統

以下任何系統：

Windows XP/2000/2003/Vista

BigFix Agent：

以下所有系統：

Windows

Mac OS X

Solaris

IBM AIX

IBM zLinux

HP-UX

VMware ESX Server

Red Hat Enterprise Linux

SUSE Linux Enterprise

Red Hat Linux

Fedora Linux

注意：功能因支援的平台不同可能有差異。關於支援 OS 版本資訊的更新列表，請查看 http://support.bigfix.com。

基於主機/基於掃描的設定管理

	基於主機	基於掃描
資料深度	可全面、即時地連結不能通過外部系統 API 提供的資訊	只能有限地連結可通過外部系統 API 提供的資訊
評估和執行	• 持續地評估並自動執行策略 • 可減少由於設定更改產生風險的可能性 • 可於線上或離線的系統上評估並執行	• 定期掃描只能提供非即時的快照 • 由於缺乏可見度會導致風險的增加 • 只能掃描在企業網路上可以看到的部分
網路及系統需要	• 實際上不影響網路效能 – 只有在發現設定變化時回應 • 具備調節能力，對系統性能影響最小	• 只能通過分割小批的流量的處理，以減少對網路及系統的整體影響 • 不能對使用和評估進行限制，可能嚴重影響系統效能
安全風險	解決方案具備適當的許可，不需要特殊的設定來實現遠程連接	需要外部認證和設定來實現遠端連接的特權訪問