tripwire SYSTEX 精誠資訊 DATASHEET

Tripwire Enterprise 8.7

偵測、應變、預防

Tripwire在安全與合規行業有近二十年的經驗，具備提供網路威脅偵測、快速和即時應變以及防止未來攻擊的基礎技術。

Tripwire Enterprise協助了一半以上的的Fortune500強企業並世界上許多對安全與合規最敏感的網路，並滿足它們在資安和政策合規上的需求。

Tripwire® Enterprise 是一個安全組態管理(SCM)套件，全面整合資安政策、檔案完整性、與矯正管理模組。企業可以一起使用這些解決方案來構建一個完整的端到端SCM解決方案，另外也可運用檔案完整性監控或政策管理解決方案來對應現今緊迫的安全與合規挑戰，同時為未來建立一個安全基礎。Tripwire的套件可以讓IT安全、合規、IT營運隊通過減少攻擊面，提高系統完整性並提供持續合規，在IT環境中快速實現安全基礎。此外，由於TripwireEnterprise可以與企業應用程式整合來將流程自動化，例如與其他的安全解決方案（如SIEM和變更管理工具），企業便可拓寬其安全視野並獲得更高的效率。

作為一個關鍵的企業資訊安全與合規解決方案，Tripwire Enterprise的偵測 、反應 、預防策略可透過以下技術落實：

» 通過凸顯可能的入侵指標來**偵測**網路威脅和可能的違規行為。

» 面對成千上萬的異動資訊提供有效**應變能力** - 高價值、低雜訊的告警，並提供如何讓系統復原到安全狀態的修復指南。

» 通過對威脅和變化的適應與優先化過程來**預防**問題發生，從而保持對所有設備和系統的持續強固與總體安全狀態。

系統如何運作
緊密整合的控制項目

Tripwire Enterprise提供四個整合功能，建立了企業級的SCM解決方案：

» **Tripwire檔案完整性管理員 (FIM)**是世界上第一個也是最好的檔案完整性監控解決方案。它能檢查大量的異質性環境，以提供威脅偵測和組態漏洞的即時資訊，同時通過減少組態調整和未經授權的異動來提升管理效率。 Tripwire FIM可以單獨使用，以提供細微的端點情資，使管理人員快速了解安全與合規狀態。如果和Tripwire政策管理員一起使用，它便能達成變更觸發進行組態檢驗以及其他的系統配置調整動作。這將「被動」的組態檢驗轉變為動態、連續、即時防禦解決方案，可立即偵測安全組態標準和強化指南預期之外的異動。

» **Tripwire政策管理員**針對超過650多種平台組合，提供安全與合規政策、標準、法規、供應商指南，建立和維護一致的agent和agent-less持續性組態檢驗。政策管理員還提

供完整的資安政策設定、豁免和異常管理、自動修復選項，以及具有門檻值、權重、嚴重性的優先級策略評分。這一切都為稽核人員提供了合規證據，並使合規團隊的政策狀態具有高度可見性和可操作性。

» **矯正管理員**是Tripwire政策管理員的增值元件，它為IT安全及合規團隊提供內建的矯正指南，方便修復偏離標準及不一致的安全組態配置，同時保留基於角色的管理、審核及修復簽發。這能使維運團隊更輕鬆、更有效地了解錯誤發生的原因，以及如何將系統恢復到正常的營運狀態。一旦達到合格的營運狀態，就不要輕易讓組態配置發生變動。

» **Investigation and Root Cause** 的下拉功能使IT安全和營運團隊能夠快速且有效地調查並確認根本原因。隨著企業不斷調整他們的人事、流程、技術，系統必然需要跟著改變。Tripwire Enterprise可以提供細微的下鑽、並排比較、歷史基線和比較等功能，方便快速提供調查團隊一切所需的資訊，如：什麼改變、何時、由誰和頻率，以及「如何」。

» **Tripwire Axon®**平台支援在各種設備、雲端和虛擬資產上進行靈活的資料收集和彈性溝通。 Tripwire Axon平台解決了資訊收集常常遇到的挑戰，通過可擴展和高效能agent、異步訊息傳遞技術以及產品和平台中性訊息定義。Tripwire Axon Agent及其插件旨在高效運行，對整體系統資源利用率和網路頻寬進行了最佳的優化。整套Agent的執行程式運用C++的語言優勢來大幅減少收集資訊的佔用空間並提供最佳的性能。

業界領先的IT安全與合規功能

Tripwire不斷為Tripwire Enterprise添加新功能，以應對不斷變化的安全性和合規性挑戰。 Tripwire Enterprise現在具有監控雲資產，保護工業設備以及使用MITRE ATT&CK框架發現環境中惡意行為證據的新功能。

» **雲管理評估器**
Tripwire的雲管理評估器能協助Tripwire Enterprise使用者確定其Amazon Web Services (AWS)、Microsoft Azure、 Google Cloud Platform的安全狀態，運用基於最佳實踐（如Center for Internet Security AWS Foundations v1.1.0 Benchmark）的資料收集、分析、評分配置資料。
此外，Cloud Management Assessor可以自動評估您的AWS S3存儲和Azure存儲，以確定它們是否暴露於匿名存取，並提供最近被暴露的標的報告。

» **Tripwire資料收集器**
Tripwire資料收集器將Tripwire Enterprise的異動偵測和政策合規性等核心功能擴展到工業環境中。監控運營技術（OT）環境有其獨特的挑戰，Tripwire資料收集器的無代理架構從一開始就設計用於評估配置、安全性和狀態，包括韌體、硬體版本、軟體版本，補丁級別等。
Tripwire資料收集器能夠通過各種工業用通訊協議與設備進行通訊，例如Modbus TCP，乙太網路/IP CIP和SNMP。對於無法連線的設備，可以通過與Rockwell自動化的FactoryTalk AssetCentre、MDT AutoSave、Kepware的KEPServerEX整合來收集配置資訊。另外還可以使用Web Retriever收集配置資料，Web Retriever可以從Web頁面中抓取配置資料。

» **MITRE ATT&CK 框架**
由MITRE公司開發的ATT&CK框架是一個好用的網路安全模型，用於說明惡意攻擊行為，並解釋您應該使用的何種策略來降低風險並提高安全性。使用Tripwire Enterprise的ATT&CK Framework政策，您可以偵測並報告環境中的惡意行為。ATT&CK規則允許您為的安全策略添加一層全新的防禦。

Tripwire運用其原有的基於主機的入侵檢測工具（即檔案和目錄的異動偵測功能），並將其擴展為強大的檔案完整性監控（FIM）解決方案，能夠監控詳細的系統完整性：檔案、目錄、機碼、配置參數、DLL、通訊埠、服務、通訊協議等。企業整合提供精細的端點智能，支援威脅偵測以及政策和稽核合規性。多年來，我們一直致力於通過政策和安全風險優先級排序，以及整合能力的提升來實現Tripwire偵測和判斷異動的能力，以實現高價值、低雜訊警報的絕對競爭優勢。Tripwire Enterprise可幫助大型企業管理系統配置的完整性、安全性、合規性。

特點和好處

更新了資料收集和通訊平台	Tripwire Enterprise的Tripwire Axon是一個安裝後無需重啟、可擴展、高效能的端點資料收集和通訊平台，提供了一流的安全性、完整性監控以及配置與合規性管理。使用者可以享受業界最佳的可見性和網路彈性，同時減少運營負擔並提高應變能力。
支援混合環境	Tripwire Enterprise可以監控內部部署環境和雲環境，以確保安全性和合規性。通過為兩種環境使用單一的解決方案，企業可以降低管理成本並擁有更好的可視性。
適用於所有IT配置的單點控制	Tripwire Enterprise提供對整個物理和虛擬IT基礎架構（包括伺服器和設備、應用程式以及多個平台和作業系統）的配置的集中控制。
通過REST API進行進階整合	更新的Rest API允許Tripwire Enterprise與其他應用程式整合。Rest API支援程式指令和對Tripwire Enterprise等應用程式的控制，以及需要收集的資訊。管理功能的API允許自動執行任務，例如啟用即時監控或執行政策檢查。
OT網路監控	通過Tripwire資料收集器與Tripwsire Enterprise搭配使用，使用者可以監控其工業網路的變更和合規性，從而在不影響可用性的情況下實現更安全的環境。
強大的資產視野功能	資產視野允許您使用與業務相關的標籤對資產進行分類，例如風險、優先級、地理位置、監管政策等。Tripwire Enterprise的資產視圖功能現在提供資產標籤檔案的功能，大量資產的擴展規模以及與Tripwire IP360整合的導入資產標記，從而更清晰地了解整個組織的風險。
用於管理失敗配置的工作流程工具	矯正管理員模組提供基於角色的工作流程工具，允許使用者核准、拒絕、推遲、執行失敗配置的修復。
與變更管理系統整合	由於Tripwire Enterprise與領先的變更管理系統（CMS）解決方案整合，因此變更發生時，Tripwire Enterprise可以自動將異動資訊與變更單和需求單勾稽。
更快、更簡單地迎接稽核	Tripwire Enterprise通過提供連續、全面的IT基礎架構基線和即時異動偵測，以及內建智能來判斷異動的影響程度，可以大幅減少稽核準備工作的時間和精力。
維持在安全、合規的狀態	Tripwire Enterprise將配置檢測與即時檔案完整性監控（FIM）相結合，可在發生異動時進行偵測、分析、報告，並使配置持續處於合規。通過即時取得的異動資訊，IT人員不用在發生重大資料外洩、稽核缺失、長時間服務中斷後才進行補救，而是在問題發生前便可把問題根源徹底解決。
自動化IT合規流程	Tripwire Enterprise可自動遵守行業法規和標準，企業現在可以遵守GCB、PCI、ISO 27001、NERC、SOX、FISMA、DISA和其他許多標準。

企業支援

Tripwire Enterprise同時支援代理及無代理操作，包含：

» **主要作業系統：**
Windows、Red Hat、CentOS、Ubuntu、SUSE、Debian

» **特定供應商作業系統：**
AIX、Solaris、HP-UX等

» **目錄服務：**
Active Directory、LDAP等

» **網路裝置：**
防火牆、IPS、IDS配置，路由器等

» **資料庫：**
Oracle、MS SQL、DB2、PostgreSQL

對IT環境的縱深支援

無論IT需要密切關注重要伺服器還是整個IT基礎架構（包括虛擬化環境和應用程式），Tripwire Enterprise都能夠檢驗、驗證、實施策略，並偵測所有來源的變更。Tripwire支援IT環境中的以下元件。

Tripwire Enterprise支援完整的服務

應用程式	Tripwire Enterprise提供合規政策管理和檔案完整性監控功能，幫助確保應用程式有正確的配置，並維持在安全、合規、最佳效能核可用程度上。
目錄服務	Tripwire Enterprise為符合LDAP的目錄伺服器對象和屬性（如LDAP schema、密碼配置、使用者權限、網路資源、群組更新和安全政策等）提供獨立的合規政策管理。
資料庫	Tripwire Enterprise運用Tripwire的檔案系統代理，幫助企業將其Oracle、Microsoft、IBM資料庫伺服器置於安全、持續高效能的狀態。
檔案系統和桌面	Tripwire Enterprise檢查物理和虛擬伺服器以及桌面檔案系統的配置，包括安全設置、配置參數和權限。
銷售點（POS機）	Tripwire Enterprise可以保護POS機免受網路威脅，管理這些設備的安全性和合規政策，並在發現疑似違例指標或「IOC」的情況下為這些設備發出警訊、通知，並提供反應指南。
虛擬化環境	Tripwire Enterprise適用於虛擬化環境，無論是私有雲、公有雲、混合雲。 Tripwire Enterprise控制台可以運行在虛擬機上，其代理可以監控任何支援的虛擬化端點，提供虛擬化/雲環境中的網路威脅提供保護、系統完整性監控、安全和合規政策的應用、儀表板、報表以及即時警報和通知。
VMware	Tripwire Enterprise提供對VMware虛擬基礎架構的可視性，實現對虛擬環境的持續配置控制。
網路設備	Tripwire Enterprise能支援業界最廣泛的網路設備的配置設定，包括運行符合POSIX標準作業系統的任何設備。

SYSTEX 精誠資訊

如需瞭解有關Tripwire解決方案的更多訊息，請訪問 www.tripwire.com 或聯繫您的精誠資訊代表。

聯絡人：林小姐
電　話：02 77201888 分機 5288
郵　件：vickylin@systex.com
地　址：台北市內湖區瑞光路318號