CIMCOR

CimTrak 技術摘要

當您的企業或機構需要確保您的 IT 基礎設施的完整性和法規遵循時，請找 CIMTRAK

作為完整性驗證和保證領域的領導者，CimTrak 幫助全球的組織與政府機構維護其關鍵 IT 資產的安全性、完整性、法規遵循與可用性。憑藉領先業界的產品和服務的成功記錄，CimTrak 不斷為市場帶來新的想法和解決方案。

為什麼選擇 CimTrak？

CimTrak 受到各種規模的組織（包括眾多財富 500 強公司）的信賴，為使用者提供功能齊全的檔案完整性監控解決方案，易於安裝、設定和管理，有別於許多 FIM 解決方案的昂貴預算與複雜性。 CimTrak 獨特的新一代檔案完整性管理 (FIM) 技術意味著您可以在更短的時間內完成更多工作，為您的組織節省時間和金錢。在世界一流的支援團隊的支持下，CimTrak 使用者可以放心，他們的系統始終處於持續完整性的狀態。

整個 IT 環境的異動偵測

CimTrak 涵蓋的基礎架構如伺服器、工作站、虛擬機器、網路設備、虛擬機器管理程式 /ESXi、容器、雲端服務、資料庫、目錄服務等。CimTrak 是單一收集點的解決方案，報告可能影響運營、安全性和法規遵循的異動。

發生異動時即時通知

CimTrak 可以讓您深入了解您的 IT 環境中正在發生的情況。持續管理並了解異動是否為已知、預期和授權，使您能夠立即找出惡意或規避的異動。這使組織能夠檢測零日漏洞及人為錯誤的問題，確保可信任的操作環境並防止完整性改變。

自動修正措施

能夠快速反應可能導致系統崩潰及業務停滯的異動是至關重要的，CimTrak 無論您的管理權限，讓您能夠立即採取自動操作來完全修復或防止異動。

產品特性

> 快速偵測惡意事件
> 深入了解系統的狀態
> 提高情境的感知能力
> 減少事件反應時間
> 改善安全狀況
> 降低補救成本
> 支援連續監控
> 有助於法規遵循工作
> 易於使用
> 設定簡單
> 動態威脅反應
> 自動復原功能

至關重要的檔案完整性

當發生意外異動時，能夠辨別異動檔案是好還是壞是非常重要的。這項困難且常令人沮喪的任務，現在可以透過 CimTrak 的可信任檔案註冊表™ (TFR) 快速而簡單地執行。TFR 是世界上最大的白名單資料庫，是由軟體供應商確保目前或異動的檔案是可信任，可提供附加資訊和完整性保證。

提供所有異動的完整報告

CimTrak 提供 IT 環境異動的完整報告、用於確認異動是好 / 壞的過程以及所採取的措施。這份完整的報告可以進行異動追蹤和驗證、稽核和法規遵循報告，以及執行級別報告。 CimTrak 可以輕鬆地將收集到的異動資訊匯出到許多企業和政府機構中的各種報告和警報工具，包括安全資訊和事件管理 (SIEMs)、安全編排、自動化和回應 (SOARs) 以及 IT 服務管理 (ITSM) 平台。

了解更多產品資訊，請洽：台灣地區代理商
商丞科技股份有限公司 (02) 2914-8001

CimTrak 如何運作

CimTrak 透過檢測檔案與設定的新增、刪除、與修改來運作。在初始設定時，CimTrak 拍攝您需要監控的檔案與設定的「快照」snapshot，並安全地儲存在 CimTrak 主儲存庫 Master Repository 中。

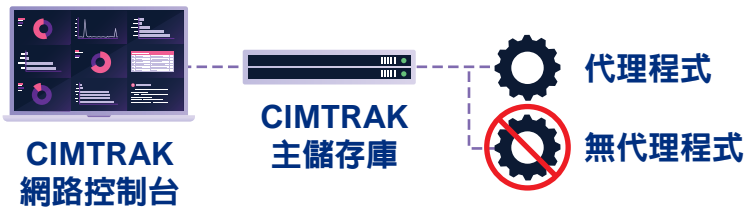
建立一個已知的良好、可信的基線。CimTrak 從各種 CimTrak 代理程式 agents 與模組 modules 接收資料。當收到的模組、特定檔案與設定加密 hash cryptographic 不一致時，意味發生了異動，CimTrak 將根據 CimTrak 的設定方式採取措施。透過 SMTP 和系統日誌發送警報，並根據需要進行即時或手動異動復原。CimTrak 主儲存庫安全地儲存檔案和設定，並執行比較以檢測異動。如果不需要此異動，則可以手動或自動反轉異動、復原到之前可信任的狀態。

代理程式與模組

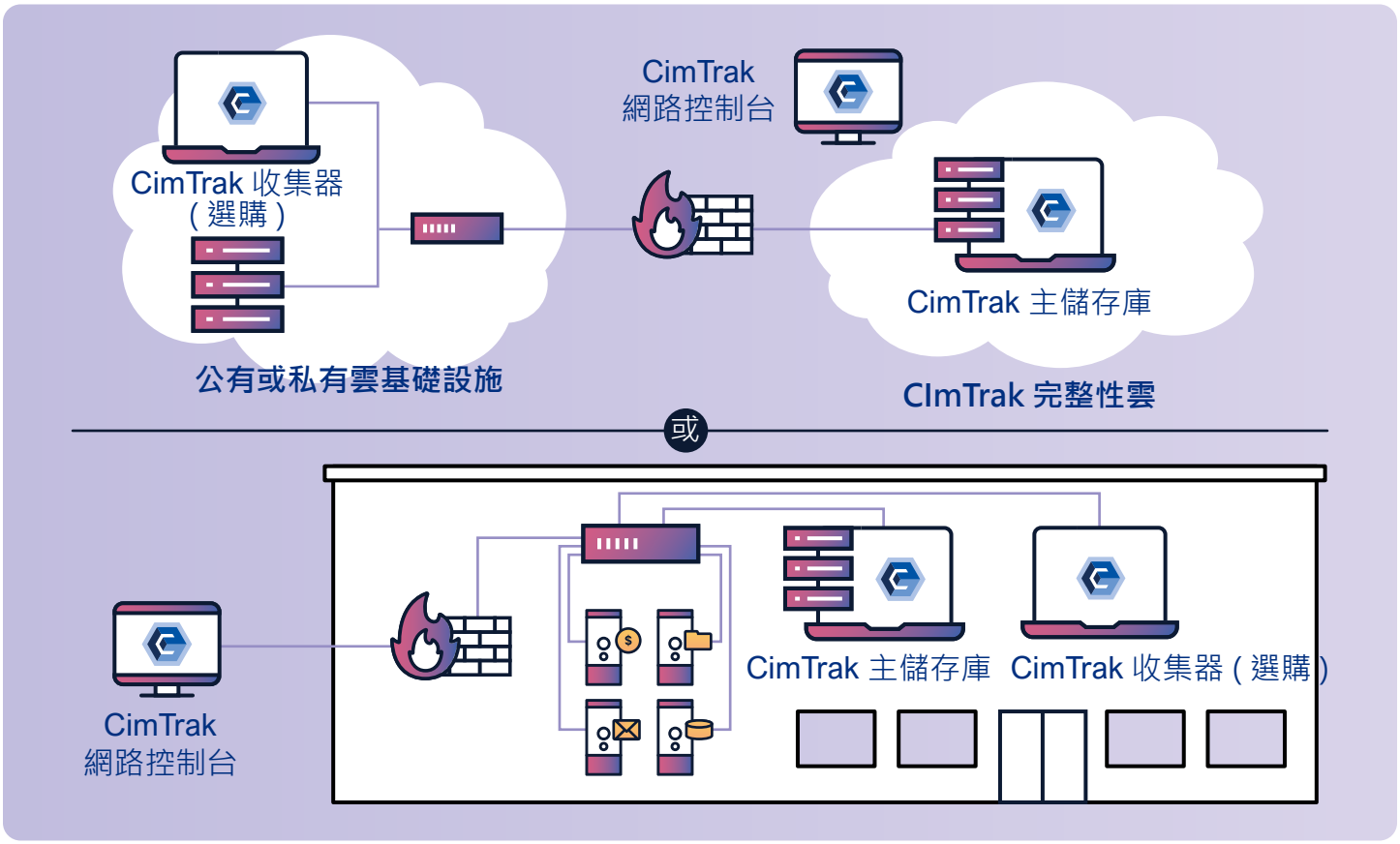
CimTrak 支援 IT 環境中的各種系統、設備和應用程式。CimTrak 根據您的特定業務和技術需求提供代理和無代理 Agentless 解決方案。

管理控制台

CimTrak 管理控制台支援多個用戶以及多租戶 Multi-Tenant 檢視，來建立所有 CimTrak 政策、程序和報告。



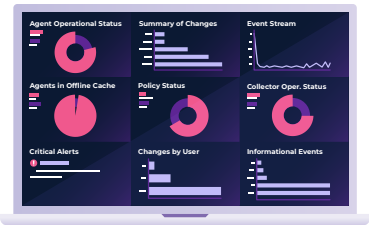
CimTrak 可在本地或雲端使用



* CimTrak 收集器的技術需求包括：
網路設備、容器編排、虛擬系統和法規遵循模組

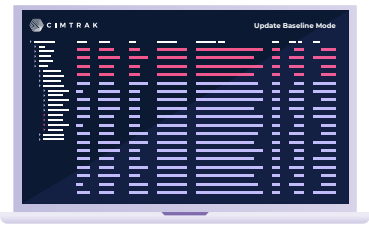
了解更多產品資訊，請洽：台灣地區代理商
商丞科技股份有限公司 (02) 2914-8001

CimTrak 操作模式



Log 日誌

Cimtrak 記錄被監控系統與應用程式的所有異動，並可進行分析和報告。

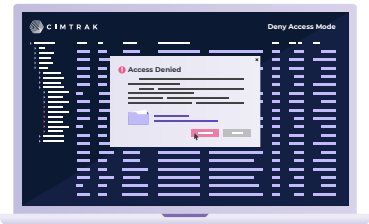


UPDATE BASELINE 更新基線

CimTrak 儲存發生異動時檔案與設定的增量「快照」incremental "snapshot"，當發生異動時，可以立即查看，以便對異動前後進行比較，此功能允許隨時分析快照和先前基線的異動。

RESTORE 自動復原

CimTrak 具有偵測到異動時立即採取反轉異動的能力，無論異動是新增、修改或刪除。可有效地允許系統「自我修復」self-heal 並實現彈性基礎設施，CimTrak 是唯一具有這種強大功能的完整性工具。



DENY RIGHTS 拒絕權限

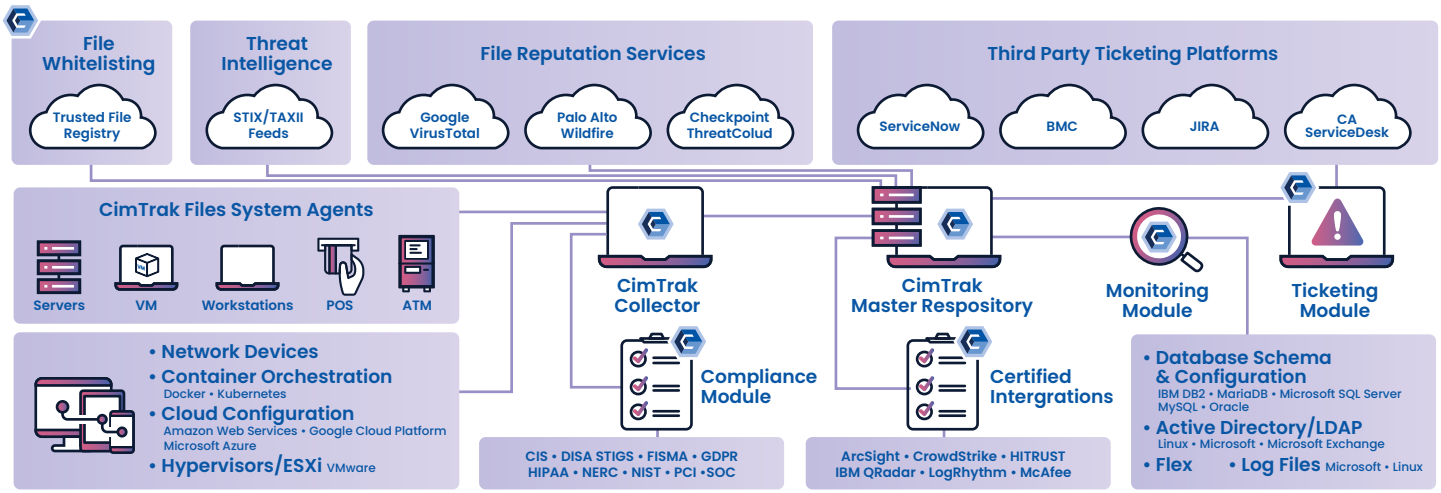
拒絕任何檔案異動，由於 CimTrak 使用本地系統帳號 local system account 執行，因此無論使用者具有什麼存取權限都不被允許異動檔案，如檔案更改、刪除或新增，沒有其他完整性工具提供這種進階功能。

值得注意的是，CimTrak 在使用各種模式時可以提供很大的靈活性。您不會被限定每個檔案或設定只使用一種模式。相反的，您可以根據異動類型選擇 CimTrak 應執行運行的模式，例如您可能希望簡單地記錄特定檔案的異動，但如果該檔案被刪除，可以將檔案恢復。

CimTrak 是安全的

基於政府客戶的嚴格需求，CimTrak 已獲得通用標準 EAL Level 4 + 認證，該認證是商業軟體產品的最高政府認證。此外 CimTrak 加密模組已通過認證並符合美國聯邦資訊處理標準（FIPS）140-2 Level 2 要求，並在美國國防部認證的產品列表中列出，這是 IT 安全產品的精英名單。

此外，您的關鍵資料是安全的，CimTrak 在元件之間的所有傳輸都完全加密，CimTrak 主儲存庫以壓縮與加密的形式儲存您的檔案或設定，沒有其他的完整性和法規遵循工具有搭配這些嚴格的保護措施來保護您的資料。無論您是政府機構還是商業企業，您都可以放心，因為 CimTrak 是安全的！



CimTrak 產品

CimTrak 安全元件

CIMTRAK 適用於伺服器

CimTrak for Servers 監控實體、虛擬或在雲端伺服器上執行的檔案和應用程式。 CimTrak 能夠在大多數作業系統上即時偵測異動，為您提供即時偵測和警報功能。此外，CimTrak 還監控安全性政策、Windows 登錄檔、系統設定、驅動程式、已安裝的軟體、連接埠、服務、使用者和群組。 CimTrak 甚至可以偵測檔案何時被開啟。 CimTrak 使用最小 CPU 資源與網路頻寬為您的 IT 環境提供最完整的解決方案。 CimTrak 與所有領先的 SIEM 解決方案整合，包括 HP ArcSight、IBM QRadar、McAfee Enterprise Security Manager、RSA Security Analytics 和 Splunk，這些都無需任何複雜的配置或設定。

CIMTRAK 適用於工作站 / 桌上型電腦

可以監視具有特定功能或執行某些關鍵應用程式的工作站與桌機。這些存在於許多環境中，包括飯店、餐廳、能源與製造業。CimTrak for Workstations / Desktops 允許您監視與 CimTrak for Servers 相同的所有項目，但是將規格縮小以滿足較小機器的需要，包括使用最少的系統和網路資源。

CIMTRAK 適用於銷售點 (POS) 系統

CimTrak for Point of Sale Systems 在您的支付卡環境中增加了 POS 系統的支援。作為您的支付卡基礎設施不可或缺的一部分，保護這些系統有助於確保客戶的支付卡資料的安全性。CimTrak 為您提供最完整的支援，以確保他們的安全與穩定的完整性狀態。

CIMTRAK 適用於 ATM

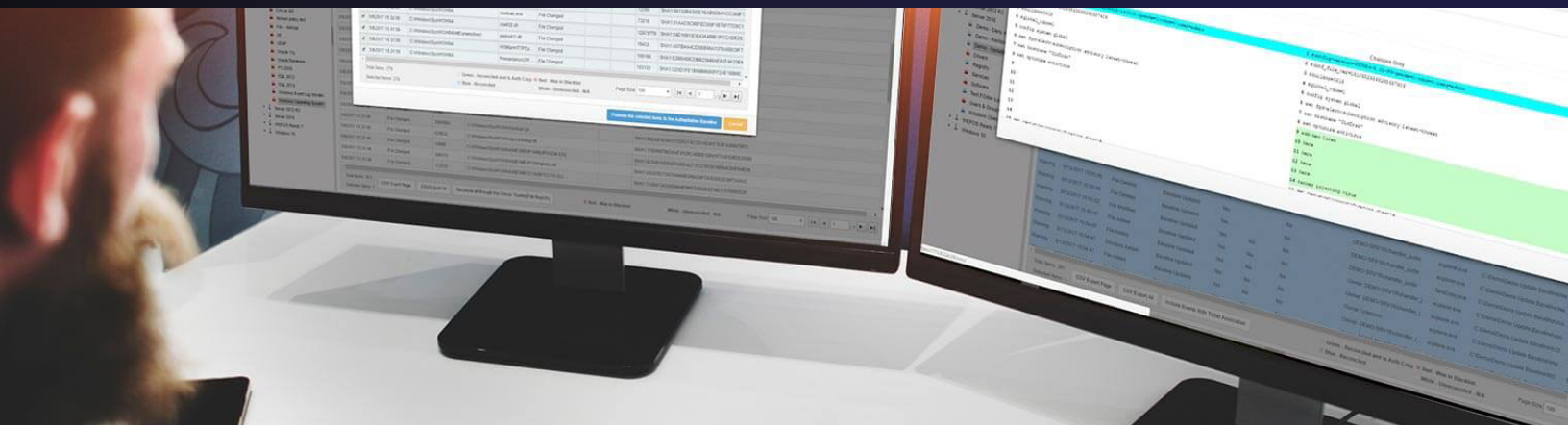
CimTrak 提供輕代理 light agent 來幫助監控和保護自動櫃員機 (ATM)，自動櫃員機很難和其他 IT 設備在相同的周期內更新和修補。CimTrak 透過確保自動櫃員機的完整性，同時提供授權和未授權異動的追蹤，提供了額外級別的威脅緩解。

CIMTRAK 適用於網路設備

CimTrak for Network Devices 偵測並提醒您關鍵網路設備上的設定異動，包括路由器、交換機和防火牆。 由於這些設備通常是進入您網路的關口，無論是惡意還是意外的異動都可能非常有問題。CimTrak 甚至可以立即復原 Cisco IOS 的設定異動。

CIMTRAK 適用於資料庫

CimTrak for Databases 為您的 IT 環境增加了另一層安全性。支援包括 Oracle、IBM 與 Microsoft 在內的主要平台，CimTrak 可確保您的關鍵資料庫的設定、用戶角色、權限以及存取設定不會偏離其已知的受信任狀態。透過使用 CimTrak for Servers，您可以進一步監視資料庫應用程式，以獲取可能影響營運的關鍵資料庫異動。



CIMTRAK 適用於目錄服務

CimTrak for Active Directory / LDAP 監視目錄服務，以查找對象、屬性和架構的偏差。大型環境可能遭受監視外的改變。由於採用分層設計，意外的異動可能僅限於單個實體，例如增加新帳號、或者拒絕服務 Denial of Service。CimTrak 提供在發生此類偏差時快速偵測、警報與復原所需的意識。

CIMTRAK 適用於虛擬設備

CimTrak for Hypervisors 監控和監督 VMware ESXi 和 Microsoft Hyper-V 的關鍵核心設定，例如用戶 / 主機存取權限、Active Directory 領域、網路設定、整合的第三方工具與進階使用者設定。由於虛擬機管理程序通常運行許多虛擬機，因此意外或惡意異動可能會迅速削弱組織的 IT 基礎設施。CimTrak for Hypervisors 使您能夠主動保護關鍵的 ESXi Hyper-V 應用程序並確保您運營的安全性和連續性。

CIMTRAK 適用於雲端

CimTrak for Cloud 提供簡單的方式來了解何時配置雲端伺服器、伺服器設定異動、虛擬防火牆規則、虛擬網路設定等。CimTrak for Cloud 支援 Google Compute Engine、Azure 和 Amazon AWS.。CimTrak for Cloud Infrastructures 讓您監控除了 Guest 作業系統外，所有的雲端基礎架構異動。

CIMTRAK 適用於容器

CimTrak for Containers (Docker / Kubernetes) 幫助管理者了解容器設定何時異動、新的容器 Containers 實例化、虛擬網路設定異動、儲存設定異動等。CimTrak for Container 提供容器 Containers 部署的設定。

CIMTRAK 適用於 FLEX 模組

CimTrak Flex Module 允許監視寫入指令的應用程式與腳本的輸出，例如 ipconfg / ifconifg 網路設定、防火牆設定、安全增強的 Linux 設定狀態等。CimTrak Flex Module 還可用於監控實體硬體狀態，如 SAN 運作狀況、以及元件與資源可用性。此外，它允許在 IT 環境中快速開發自行定義的應用程式監視工具。通過偵測對腳本 / 應用程式輸出的任何異動，可以立即提醒和反應偏差。自動監視與分析自行定義腳本或指令執行，簡化 IT 操作，使人員能夠專注於更緊迫的問題。

CIMTRAK 適用於 SCADA 設備

CimTrak 提供必要的偵測控制，協助您滿足多項關鍵 NERC-CIP 要求，並涵蓋製造、能源設施和其他工業環境中常見的各種關鍵伺服器、SCADA 設備、工作站和網路設備。相同的流程和異動偵測功能用於 SCADA 設備進行基準設定、比較和復原不必要的異動，以確保操作完整性。

THREAT INTELLIGENCE 威脅情報

CIS 基準和 DISA STIGS

CimTrak 結合使用 CIS 基準和 DISA STIGs 作為強化系統、設備、作業系統、應用程式等的可信賴來源。這些基準用於建立可參考的信任根源。當 CimTrak 識別出這些配置設定（基準）的異動時，可以立即發出異動警報並採取修正措施來復原這些異動。

STIX/TAXII

CimTrak 整合 STIX 和 TAXII 威脅情資，以提供額外的安全情報。這種持續的威脅情資讓 CimTrak 更深入了解您的組織。當新的威脅 hash 下載於威脅情資 Thread Feeds，CimTrak 會自動使用惡意軟體 / 威脅 hash 更新其黑名單。每當發生異動時，CimTrak 都會驗證這些異動或新檔案是否在黑名單上。此外，隨著新威脅的辨識，CimTrak 將主動審查所有受監控的系統，以確保新發現的威脅不存在於當前系統上。

CIMTRAK 可信任檔案註冊表™

CimTrak Trusted File Registry™ 是正在申請專利的關鍵組成技術，這種高度創新的解決方案幾乎消除其它供應商的修補程式與更新 patches and updates（例如 Windows 和 Red Hat Linux 的更新）所引起的誤報。通過自修補程式與更新授權基線 Authoritative Baseline，真正重要的異動浮出水面，大大減少調查異動所花費的時間與最大化識別和回復未知、不需要和未經授權的異動。

CIMTRAK 檔案信譽服務

當檔案發生異動時，CimTrak 可以與 Virus Total、Palo Alto Wild fire 或 Checkpoint 的威脅 API 整合，對檔案異動進行即時分析。結合 CimTrak Trusted File Registry™，現在比以往更容易識別檔案是否是惡意的。此資料可用於動態更新 CimTrak 黑名單 Blacklist，並自動檢查 CimTrak 監控的其他系統上是否存在惡意資料。

CIMTRAK 工作流程與報告

CIMTRAK 票務模組

區分已知的 " 好 " 異動和應該調查的未知異動之間的差異，是您和您的團隊能大幅度地提昇反應異動事件時間的關鍵部分。CimTrak 為用戶提供唯一的檔案完整性監控系統，可提供完全整合的雙向異動票務系統，自動化地確保只執行經過批准的信息和命令異動。這讓各種規模的組織以符合經濟效益的成本，擁有執行計劃和記錄異動的能力。CimTrak 已整合所有領先的 ITSM 解決方案雲端供應商合作，整合的異動票務系統 Change Ticketing System 允許與現有的票務解決方案整合，包括 ServiceNow、BMC、Atlassian Jira 等。

CIMTRAK 整合 – SIEM、SOAR 和 ITSM

如果您的組織使用其他安全和營運管理工具，例如 SIEM、SOAR 或 ITSM 技術，則可以輕鬆整合 CimTrak 收集的資料。CimTrak 提供來自伺服器和其他終端的資訊。CimTrak 的檔案完整性監控（FIM）和設定監控提供及時的資訊以緩解攻擊與檢測其他異常所需的分析、關聯和情況感知。通過檢測 binary 二進制、設定與系統狀態的實際異動，CimTrak 補足了網路流量分析解決方案可能會錯過的事件。

透過 CimTrak 的完整性管理資料能力增強可監控的安全控制覆蓋範圍，以擴展 SIEM 和 ITSM 的法規遵循報告。CimTrak 提供前所未有的捕獲證據輔助細節，還為 SIEM 的強大的數據挖掘引擎 Data Mining Engine 以及 SOAR 自動化回復功能增加重要資訊。

CimTrak 與這些技術的整合可以幫助簡化法規遵循報告、提高您的安全狀態、確保營運可用性，並符合 CIS Controls、HITRUST、NIST 800-53 等眾多控制目標。

CimTrak 整合所有領先的 SIEM/SOAR 解決方案，包括 HP ArcSight、IBM QRadar、McAfee Enterprise Security Manager、RSA Security Analytics 和 Splunk，且都不需任何複雜的配置或設定。 CimTrak 整合領先的 ITSM 框架（例如 ServiceNow、BMC、Atlassian 和 CA），以建立異動管理流程。

COMPLIANCE 法規遵循

CIMTRAK 法規遵循

CimTrak Compliance Module 評估您環境中的伺服器、工作站、網路設備、POS 銷售點和其他 IT 設備的設定。透過對照既定的監管標準檢查您的設定，您可以確定系統是否符合要求，包括 SOX、PCI、HIPAA、FFIEC、FISMA、NERCCIP、SWIFT、GDPR、CDM、CJIS 等等。CimTrak 提供不符合法規的詳細報告，並提供如何快速糾正並進入符合法規狀態的說明。然後，CimTrak 將檢測並顯示之後的任何設定異動，並且會立即向指定人員發送警報。這確保了您的系統始終符合法規且安全。

CIMTRAK AS A SERVICE

CIMTRAK 完整性雲

依未來需求提供易於管理、全面性且符合經濟效益的系統，是確保完整性和驗證的解決方案。CimTrak 的服務，具有與本地部署相同的特性 / 功能，又能利用雲端運算的價值和效率。Cimcor 已與領先的雲端供應商合作，以減輕部署、操作和維護的負擔，具有成本效益又可立即實現。

大規模管理您的環境：CIMTRAK 功能

CIMTRAK 整合式儀表板

CimTrak 的互動式圖形儀表板允許 CimTrak 使用者一目了然地查看其環境的狀態。此外每個使用者可以自行定義其儀表板，以提供獨特的圖表，允許他們快速輕鬆地查看整個 IT 環境的狀態，或只是他們負責的系統。

透過統一管理視圖輕鬆擴展

可以透過 CimTrak Clustering 將多個 CimTrak Master repositories 主儲存庫叢集在一起，以水平擴展 CimTrak。這種技術使 CimTrak 能夠滿足商業和政府最大型基礎設施的需求。叢集後 CimTrak 會自動啟用整合圖表功能，為用戶提供強大的「單一窗格」"Single Pane of Glass"，用於管理設定、建立政策以及檢查與安全相關的事件。

CIMTRAK 報告

能夠提供異動資訊報告是非常重要的，如：證明 IT 稽核的法規遵循、驗證發生的計劃異動以及讓所有 IT 運營人員了解情況。在企業中不同職能領域的個人通常需要不同詳細程度的不同報告。借助整合的報告引擎，CimTrak 提供各種 .pdf，.html 和 .csv 報告格式，用戶也可以自行定義報告內容以顯示其組織特有的資訊。從全面詳細的更改報告到高級概述報告（適用於管理演示），CimTrak 可為您提供組織所需的各種級別報告。

CIMTRAK 異動協調工作流程

使用 CimTrak 可以更有效地管理企業範圍內的異動。CimTrak 異動調節工作流程 Change Reconciliation workflow 提供了一種無縫、易於使用的方法，從最初識別異動、調查與異動分類、將任務分配給工程師、最終補救與確認。CimTrak 異動協調工作流程提供了一個強大的工具集，用於分析異動的性質、執行惡意軟體分析、驗證異動是否為作業系統修補程式 OS patch 的驗證元件、記錄已完成操作及由誰執行操作的簡單方法。

SUPPORTED PLATFORMS 支援平台

CimTrak for Servers, Critical Workstations & POS Systems 伺服器、關鍵工作站和 POS 系統

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise
WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022
LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others
FreeBSD 12, 13
SUN SOLARIS x86/SPARC
MacOS 5, 6, 7, 8, 9, 10, 11
HP-UX Itanium, PA-RISC
AIX 6.1, 7.1, 7.2, 7.3

Windows Parameters Monitored Windows 監控參數

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES Compressed, hidden, offline, read-only, archive, reparse point, Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored UNIX 監控參數

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices 網路設備

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases 資料庫

IBM DB2, Microsoft SQL Server, MySQL, Oracle
PARAMETERS MONITORED Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors 虛擬設備

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms 雲端平台

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations 支援的容器與編排

Amazon Elastic Kubernetes Service (EKS), Docker, Docker Enterprise, Google Kubernetes Engine (GKE), Kubernetes, Podman

Supported Ticketing Integrations 票務模組

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations SIEM 模組

IBM QRadar, LogRhythm, McAfee Event Security Manager, Microfocus Arcsight, Splunk, others

Supported Under CimTrak's Trusted File Registry™ 檔案白名單

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

SUPPORTED BENCHMARKS 支援基準

ALIBABA
ALMA
AMAZON ELASTIC KUBERNETES
AMAZON LINUX
APACHE
APPLE MAC OS
AZURE
CENTOS
CISCO Firewall, IOS
DEBIAN
DISTRIBUTION INDEPENDENT
FEDORA
GOOGLE Chrome, Container, Kubernetes
IBM
KUBERNETES
MICROSOFT Access, Edge, Excel, IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word
MONGODB
NGINX
ORACLE Cloud, Database, Linux, MySQL
PALO ALTO
POSTGRESQL
RED HAT
RHEL8
ROCKY
ROS
SUSE
UBUNTU LXD, Linux
VMWARE

CIMCOR

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

REQUEST A DEMO

CIMTRAK

CIMCOR.COM | FOLLOW US @CIMTRAK
了解更多產品資訊，請洽：台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001