InTrust®

聰明且可擴充的事件記錄管理工具

對貴組織來說，擁有的資料以及有權存取資料的使用者都是最寶貴的資產。而對 IT 和資安部門而言，爲維護環境安全及遵循多項產業法規，追蹤使用者和權限帳戶活動 (特別是工作站或使用者裝置的活動) 就是他們最重要的工作。然而，由於有大量資料分別儲存於不同的系統、裝置和應用程式中，要追蹤活動可說是十分艱鉅的工作。一般來說，相關部門需要準備大量儲存空間，花費許多時間收集事件資料，並具備與收集的資料相關的內部專業知識，才能收齊這類資料並進行儲存和分析工作。

透過 Quest® InTrust®，您可以監控所有的使用者工作站，同時全盤掌握從登入到登出期間的所有管理員活動。您可以 20:1 壓縮資料，大幅縮減儲存成本，並從 Windows、UNIX/Linux 伺服器、資料庫、應用程式及網路裝置中儲存累積多年事件記錄。InTrust 的即時警示功能可讓您透過自動化回應功能應對可疑活動，以便即時回應威脅。

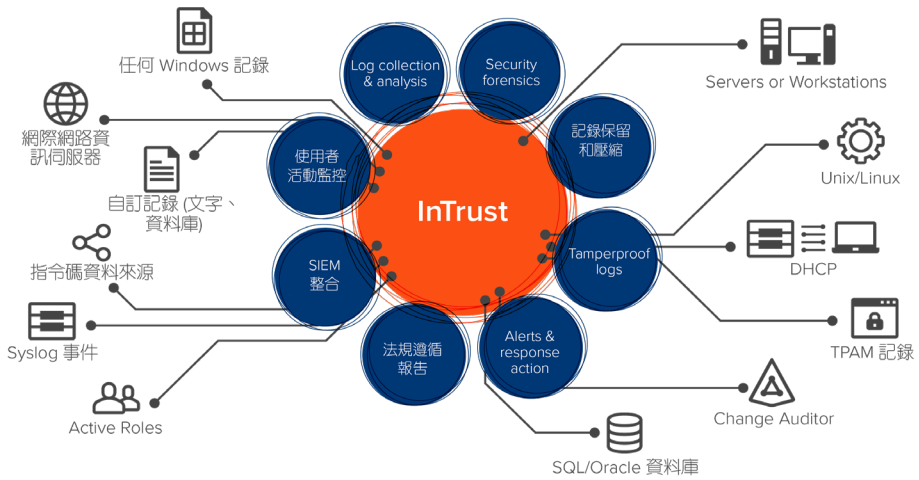
功能特色

單一窗口

從一個可搜尋的集中位置，從各種系統、裝置及應用程式中收集和儲存所有原生或第三方的工作站記錄，並可立即回報安全性和法規遵循狀況。InTrust 可集中檢視 Windows 事件記錄、UNIX/Linux、IIS 和 Web 應用程式記錄、PowerShell 稽核追蹤、端點保護系統、Proxy 和防火牆、虛擬化平台、網路裝置、自訂文字記錄，以及 Quest Change Auditor 事件

使用者工作站記錄監控

從登入到登出，全程監控使用者和管理員的活動，藉此保護您的工作站免於傳遞雜湊、網路釣魚和勒索軟體等現代化網路攻擊的侵擾。收集和儲存所有使用者存



有效監控所有使用者工作站和管理員活動，確保您最寶貴資產 (也就是您的資料) 的安全。

「我們使用 InTrust 來收集網域控制站的記錄，並監控 SOX 法規遵循稽核的事件。我喜歡這款存放庫檢視器；在我們爲資安目的研究帳戶鎖定和其他登入事件時，這項工具能發揮極大作用。」

標準普爾 500 大專業服務公司所屬工程師

TVID：726-084-5E5

優點：

- 使用高度壓縮且索引化的記錄存放庫，大幅縮減儲存成本，並確保持續遵守規範
- 在一個集中的地方輕鬆搜尋所有使用者和權限帳戶活動
- 快速回報、執行故障診斷及調查資安事件
- 透過標準化原生事件記錄，讓您的資料更有意義
- 輕鬆整合您現有的 SIEM 解決方案
- 透過即時警示和自動化回應功能，立即對威脅做出回應
- 在建立事件時加以複製，防止事件記錄資料遭到竄改或破壞

「我認爲這款產品提供的安全性報告和警示功能是無價的。雖然其他產品也有類似功能，但我仍認爲 InTrust 具備快速實行能力，可立即在稽核和法規遵循領域發揮其價值。」

財星 500 大企業，汽車及運輸公司所屬資深 IT 管理員

TVID: D2B-CDB-505

系統需求

支援的平台
Microsoft Windows 事件
Microsoft IIS 事件
Microsoft Forefront Threat Management Gateway 和 ISA Server 事件
Microsoft DHCP 伺服器事件
Solaris 事件
Red Hat Enterprise Linux 事件
Oracle Linux 事件
SUSE Linux 事件
Debian GNU/Linux 事件
Ubuntu Linux 事件
IBM AIX 事件
HP-UX 事件
VMware vCenter 事件
VMware ESX 和 ESXi 事件
如需詳細資訊，請參閱系統需求文件。

取的必要詳細資料，例如執行動作的使用者、涉及哪些動作、發生事件的伺服器，以及事件的工作站源頭。

簡化事件記錄分析

整合來自不同來源的隱密事件記錄，以簡單的標準化格式提供對象、內容、時間、地點、來源及受影響對象等資訊，協助您瞭解資料內容。尤其是 Syslog 資料，在各應用程式之間可謂大相逕庭。使用 InTrust®，您便可以偵測到結構化資料內的 Syslog 事件，並正確剖析此資料。獨特的全文索引功能，可讓您輕鬆搜尋長期事件資料，以便快速取得報告、進行故障診斷和安全調查。

聰明、可擴充的事件記錄壓縮功能

以高度壓縮的存放庫收集和儲存大量資料 (有索引的壓縮率爲 20:1，無索引爲 40:1)，可協助您節省最多%，並確保能持續遵守 HIPAA、SOX、PCI 和 FISMA 等規範。另外，一部 InTrust 伺服器每秒最多可處理 60,000 起事件，還能同時透過 10,000 個代理程式寫入事件記錄，爲您提高效率、擴充性，並大幅節省硬體成本。若您需要更多容量，只要添購新的 InTrust 伺服器，然後分割工作負荷即可，擴充性幾乎沒有上限。

即時警示和回應動作

監控未授權或可疑的使用者活動，例如：建立的檔案超過臨界值限制、使用的副檔名爲已知的勒索軟體攻擊或釣魚 PowerShell 命令，然後發出即時警示，讓您立即回應威脅。InTrust 可讓您輕鬆觸發對可疑事件的自動回應，例如：阻擋活動、停用違規的使用者、復原變更，以及/或是啓用稽核。

防竄改記錄

在每部遠端伺服器上建立快取位置，讓系統在建立記錄後加以複製，藉此防止事件記錄資料遭到竄改或破壞。

SIEM 整合

使用適用於 Splunk 和 IBM QRadar 的 InTrust 連接器，可大幅縮減每年的 SIEM 授權成本。使用 InTrust 儲存長期事件記錄資料，然後依據業界最佳作法，僅將相關資料轉送到您的 SIEM 解決方案，以便即時分析安全性。

以 IT Security Search 提升洞察能力

在一個集中的地方，從所有 Quest® 安全性與法規遵循解決方案中獲取寶貴的洞察能力。您可以透過 IT Security Search 使用類似 Google 的 IT 搜尋引擎，爲來自 InTrust、Change Auditor、Enterprise Reporter、Recovery Manager for AD 及 Active Roles 的資料建立關聯，以加快資安事件回應和鑑識調查分析速度。透過豐富的視覺效果和事件時間軸，輕鬆分析使用者權利和活動、事件趨勢、可疑模式等資訊。

自動化的最佳措施報告

輕鬆將調查結果轉爲多種報告格式，包括 HTML、XML、PDF、CSV、TXT，以及 Microsoft Word、Visio 和 Excel。爲各團隊排程報告並自動分發，或運用內建的事件記錄專業知識，從大型資料庫中選擇預先定義的最佳措施報告。藉由資料匯入及整合工作流程，您甚至還能自動轉送資料子集至 SQL Server，藉此進一步分析。

關於 QUEST

Quest 爲快速變遷的企業 IT 世界提供軟體解決方案。我們可協助簡化資料暴增、雲端擴張、混合式資料中心、安全威脅及法規要求所帶來的難題。我們的產品組合包含用於資料庫管理、資料保護、統一端點管理、身分識別與存取權管理，以及 Microsoft 平台管理的解決方案。

Quest
quest.com
請前往網站 (quest.com) 以瞭解當地辦事處的資訊。

DataSheet-InTrust-TW-KS-zh_TW-WL-39601