# InTrust®

可擴展的智能事件日誌管理工具

組織中最有價值的資產為其資料和有權限存取資料的使用者。對 IT 和資安部門而言，追蹤使用者和特權帳號的活動 (尤其是在工作站或終端使用者的設備上) 是保持企業環境安全並遵循各產業規範的核心。但這是一項艱鉅的任務，因為大量的資料分散在不同的系統、設備和應用程式中。通常需要經過大量的儲存、耗時的收集過程，以及具備內部專業知識，才能有效利用這些資料。

使用 Quest® InTrust®，您可以監控所有用戶工作站和管理員活動，包括從登入到登出，及期間的所有一切行為，透過 20:1 的資料壓縮大幅降低儲存成本，並可儲存來自 Windows、UNIX/Linux 伺服器、資料庫、應用程式、網路設備的事件日誌長達數年。InTrust 的即時警報功能可自動回應可疑活動，讓您能快速的應對威脅。

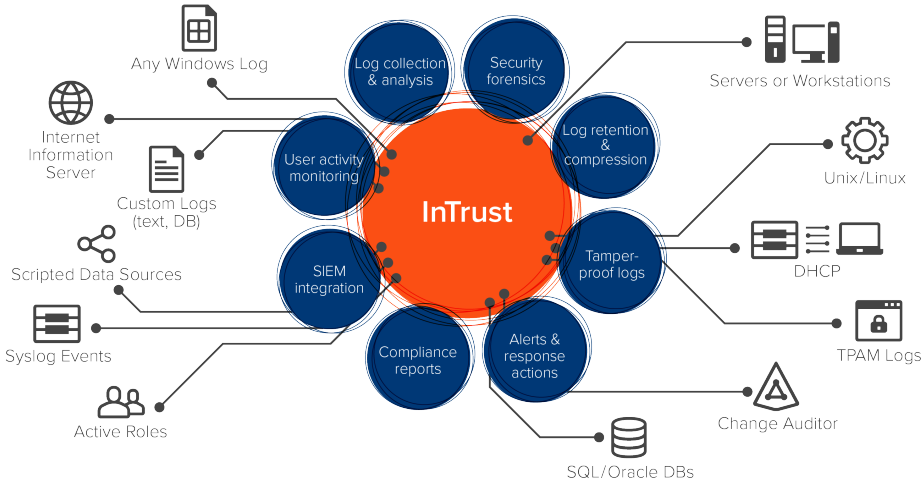
## 特點

### 集中日誌收集

透過一個具搜尋功能的平台位置，收集並儲存來自各種系統、設備和應用程式中的所有本機或第三方工作站日誌，並即時提供安全性和合規性報表。InTrust 提供 Windows 事件日誌、UNIX/Linux、IIS 和 Web 應用程式日誌、PowerShell 審核追蹤、端點保護系統、代理和防火牆、虛擬化平台、網路設備、自定義文本日誌以及 Quest Change Auditor 事件的統一視圖。

### 用戶工作站日誌監控

監控用戶工作站和管理員活動，包括從登入到登出，及期間的所有一切行為，進而保護您的工作站免於現代網路攻擊，如：哈希傳遞 (PTH)、網路釣魚、勒索軟體。收集並儲存有關使用者存取的所有詳細資訊，包括誰在何時執行什麼操作行為，在哪一台伺服器以及工作站來源。




*有效監控所有用戶工作站和管理員活動，以保護您的重要資產 – “企業資料”*

> “我們使用 InTrust 從網域控制站進行日誌收集，並監控事件以滿足 SOX 合規性審核。我喜歡儲存庫檢視器功能，它非常適合用於研究帳號鎖定和其他登入事件，以確保安全性。”
>
> *S&P 500 專業服務公司的工程師*
>
> TVID: 726-084-5E5

## 優點：

- 透過高度壓縮和已建立索引的日誌儲存庫，降低儲存成本並確保持續合規性。
- 從單一平台位置輕鬆搜尋所有終端用戶和特權帳號的活動。
- 快速的報表、故障排除和安全事件調查。
- 藉由正規化的本機事件日誌了解您的資料。
- 可與您現有的 SIEM 解決方案輕鬆整合。
- 利用即時警報和自動化回應，立即應對威脅。
- 對建立的事件日誌進行複製，防止資料被篡改或破壞。

“我相信此產品提供非常寶貴的安全報表和警報功能。儘管其他產品也提供類似的功能，但我認為 InTrust 產品定位是能夠快速執行，並在審核和合規領域即時產生價值。”

*Fortune 500 汽車及運輸公司*
*資深 IT 經理*

TMD: D2B-CDB-505

**系統需求**

| 支援平台 |
| --- |
| Microsoft Windows 事件 |
| Microsoft IIS 事件 |
| Microsoft Forefront Threat Management Gateway 和 ISA Server 事件 |
| Microsoft DHCP Server 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 |
| 更多詳細資訊，请参考系統需求文件。 |

### 簡化的事件日誌分析

將來自分散來源的加密事件日誌整合成一種簡單的標準化格式，其中包括相關使用者、內容、時間、位置，來幫助您了解日誌資料，尤其各種應用程式的系統日誌資料更是截然不同。透過 InTrust®，您可以檢測系統事件日誌中的結構化資料，並正確解析這些資料。獨特的全文索引功能可以輕鬆的搜尋過往的事件日誌資料，從而實現快速的報表、故障排除和安全調查。

### 可擴展的智能事件日誌壓縮

收集大量資料並儲存在高度壓縮的儲存庫中 (已建立索引資料以 20:1 的壓縮率，無建立索引資料以 40:1 的壓縮率)，有效減少多達 60% 的儲存成本。滿足資料保留策略並確保持續符合 HIPAA、SOX、PCI、FISMA 等。此外，一台 InTrust 伺服器每秒可以處理多達 60,000 個事件且支援 10,000 個代理程式同時寫入事件日誌，使您實現更高的效率、更大的可擴展性並節省大量硬體成本。對於需要更多容量的大型企業，只需添加另一台 InTrust 伺服器來分散工作負載，可擴展性幾乎是無限的。

### 即時警報和回應操作

監視未授權或可疑的使用者行為，例如：建立超出閾值限制的檔案、使用已知的勒索軟體攻擊的檔案擴展名或可疑的 PowerShell 命令。通過即時警報即時應對威脅。InTrust 使您可以輕鬆觸發對可疑事件的自動化回應，例如：阻止活動、禁用違規用戶、撤銷變更和/或啟用緊急審核。

### 日誌防竄改

InTrust 能讓您在遠端主機建立一個快取空間，儲存在建立事件日誌時複製產生的副本，可保護事件日誌免遭篡改或刪除。

### SIEM 整合

InTrust 支援與 Splunk、QRadar、ArcSight 和任何其他常見系統日誌格式 (RFC 5424、JSON、Snare) SIEM 的輕鬆可靠的整合，可大幅降低您的年度 SIEM 授權成本。透過 InTrust 長期收集、儲存事件日誌資料，並根據行業規範過濾資料，僅將相關日誌資料轉發到現有的 SIEM 解決方案，以進行即時安全性分析。

### 藉由 IT Security Search 提高洞察力

集中於一處管理利用所有 Quest 安全與合規性解決方案提供的寶貴洞察力。借助 IT Security Search，您可以在類似於 Google 的 IT 搜尋引擎中關聯來自 InTrust、Change Auditor、Enterprise Reporter、Recovery Manager for AD 以及 Active Roles 的資料，實現更快的安全事件回應和取證分析。透過豐富的視覺化和事件時間表，輕鬆分析使用者授權和活動、事件趨勢、可疑模式等。

### 自動最佳實務 (Best Practice) 報表

輕鬆將調查結果轉換為多種報表格式，包括 HTML、XML、PDF、CSV、TXT 以及 Microsoft Word、Visio、Excel。可排程報表並自動分送給各部門，或從內建事件日誌資訊的大量預定義最佳實務報表庫中選擇。藉由資料導入和整合工作流，您可以將資料的子集自動轉發到 SQL Server，做更進一步的分析。

### 關於 QUEST

Quest 為快速變遷的企業 IT 世界提供軟體解決方案。Quest 可協助簡化資料暴增、雲端擴張、混合式資料中心、安全性威脅和法規要求所帶來的難題。其產品組合包括資料庫管理、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
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.



DataSheet-InTrust-US-KS-40306