IT Security Search

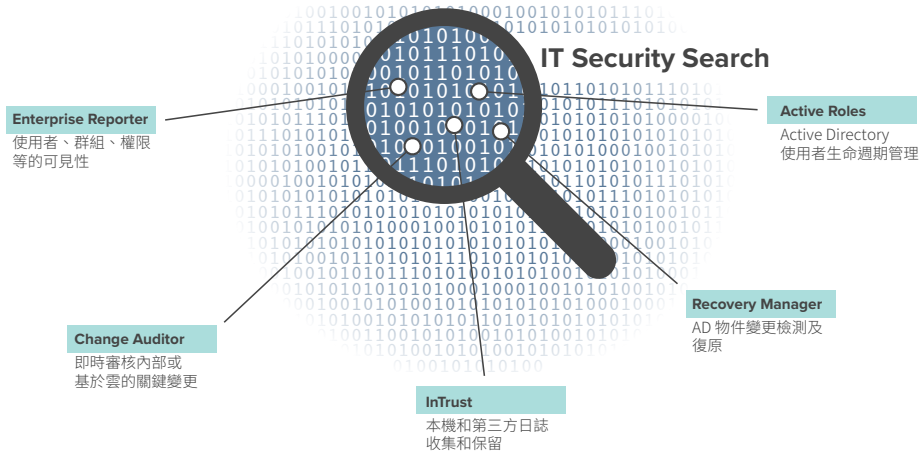
將不同的 IT 資料關聯到交互式搜尋引擎

在分散式的 IT 環境中很難持續追蹤誰擁有資料的存取權限，以及他們是如何獲得權限和使用權限。查找看不見的內容是 IT 面臨的一項挑戰。在面對各種不同來源 (地端和雲端環境) 中要收集和審核的數十億計的事件，很難找到其相關性和所包含的意義，若能在內部或外部出現安全漏洞時，確定最初發生漏洞的位置和存取的內容，則結果將會有很大的不同。在許多 Quest® 解決方案中提供的 IT Security Search 功能可以大大簡化上述工作。

IT Security Search 是一款類似於 Google 的交互式搜尋引擎，可以讓 IT 管理員和資安部門快速回應安全事件並取證分析。它透過基於 Web 的介面，將來自許多 Quest 安全與合規性解決方案的分散 IT 資料，集中至單一管理平台。

透過快速搜尋，您可以查看誰執行了哪些操作及執行的時間和位置、Active Directory (AD) 中的關鍵物件是否發生了變更、授予使用者或群組的特權是否被提升，或者是否有人不當存取了敏感檔案或資料夾資料。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。

IT Security Search 是包含在 Quest 許多解決方案 (如：Enterprise Reporter、Change Auditor、InTrust®、Recovery Manager for AD 和 Active Roles)的附加功能，可將資料集中至單一管理介面，您可以輕鬆檢視內部部署或混合環境中的所有活動行為，並執行相應的操作。配置基於角色的存取權限，提供審核員、技術人員、IT 主管和其他相關者能夠準確獲取他們所需的報表。



使用 IT Security Search，可比過往更輕鬆容易發現內部和外部安全漏洞問題。

IT Security Search 使用簡單自然的搜尋語言，來幫助管理員和資安團隊快速調查內部攻擊行為。

優點：

- 簡化對分散式獨立系統的關鍵 IT 資料的搜尋、分析和維護工作。
- 透過一個具搜尋功能的平台位置，即時、全面地查看特權使用者、伺服器和檔案資料，加快安全性調查及合規性審核的速度。
- 在發生中斷或安全漏洞時，對相關聯的問題一併進行故障排除。
- 輕鬆快速地恢復損壞或被惡意更改的 AD 物件。
- 支援基於角色的存取，為所有相關者準確提供他們所需的報表。

系統需求

相容性

此版本的 IT Security Search 可支援下列產品版本：

InTrust 11.4, 11.3.2, 11.3.1, 11.3, 11.2

Change Auditor 7.0, 6.9.5, 6.9.4, 6.9.3, 6.9.2, 6.9.1, 6.9, 6.8

Enterprise Reporter 3.1, 3.0, 2.6, 2.5.1

Recovery Manager for Active Directory 9.0.1, 9.0, 8.8.1, 8.8, 8.7.1, 8.7

Active Roles 7.3.1, 7.2.1, 7.2, 7.1, 7.0

軟體需求

作業系統：
Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

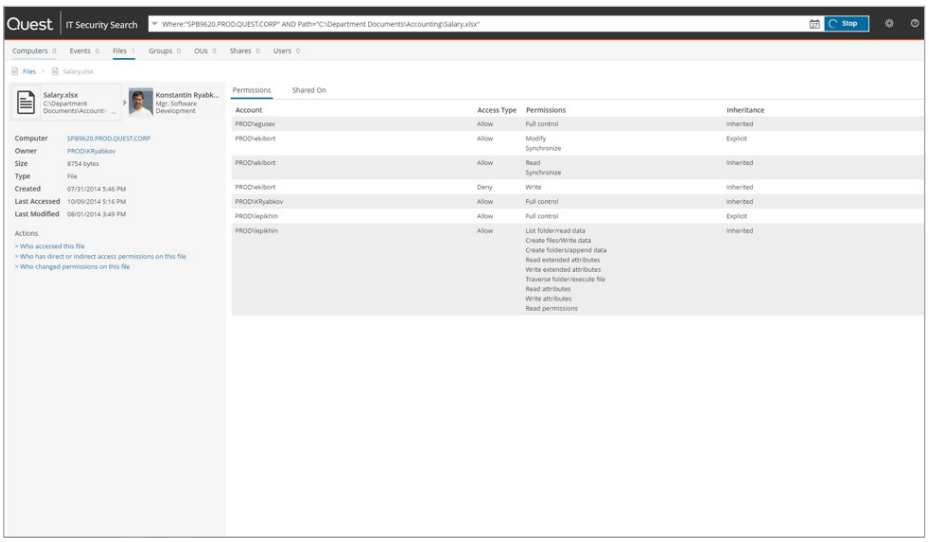
Microsoft Windows Server 2008 R2

其他軟體：
Microsoft .NET Framework 4.6.2 (含)以上版本

Microsoft Windows PowerShell 3.0 (含)以上版本

Microsoft SQL Server 2012 (含)以上版本 (all editions). 此為 IT Security Search Warehouse 元件的需求，用於進行內部配置管理。

更多系統需求的最新詳細資訊，请至 quest.com/products/it-security-search.



輕鬆了解使用者的帳號、操作行為、位置和存取方式等資訊。

基於狀態的資料 (STATE-BASED DATA)

- 藉由 Enterprise Reporter，可深入了解本地端、Azure 以及混合環境中的重要資訊，包括使用者、電腦、群組，以及群組成員身分、單位部門 (OU) 和檔案/資料夾權限、所有權等等，進一步提升 IT 團隊的能力，以全面了解其安全狀態。
- 使用 Active Roles 檢視虛擬屬性、動態群組成員、暫時性群組成員和受管理單位。

即時安全審核

- 透過 Change Auditor 搜尋有關本地端、Office 365 或 Azure AD 中關鍵物件和敏感資料的即時更改資訊。
- 補充更多本機稽核的詳細資料 (如：提出 AD 異動的實際使用者等)，即使變更是藉由Active Roles 提出的也是如此。

資料收集和日誌封存

借助 InTrust® 日誌管理，可以從各種企業網路中收集本機日誌 (Windows 伺服器、Unix/Linux、工作站等) 及第三方日誌。

壓縮且可建立索引的線上儲存庫

利用 InTrust 在長期儲存的事件日誌和其他伺服器資料中進行全文搜尋，以實現合規性和安全性，並節省了查詢事件的時間。

物件復原

透過 Recovery Manager for AD 可發現 AD 中哪些物件已被更改 (包括過往和當前的值)，並單擊點選即可將其還原。

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-ITSS-US-KS-38937